

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**IN RE: EQUIFAX INC.
CUSTOMER DATA SECURITY
BREACH LITIGATION**

**MDL Docket No. 2800
No. 1:17-md-2800-TWT**

**This document relates to:
CONSUMER CASES**

**MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS
CONSOLIDATED CONSUMER CLASS ACTION COMPLAINT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES	V
INTRODUCTION.....	1
FACTUAL BACKGROUND & PROCEDURAL HISTORY.....	5
LEGAL STANDARD & CHOICE OF LAW	10
A. Pleading requirements.	10
B. Choice of law.	11
ARGUMENT.....	12
I. THE CLAIMS PLAINTIFFS ASSERT ON BEHALF OF A PUTATIVE NATIONWIDE CLASS ARE DEFECTIVE AND MUST BE DISMISSED.....	12
A. Plaintiffs’ Fair Credit Reporting Act Claims Must Be Dismissed.....	12
1. Equifax Did Not “Furnish” Any Information To The Criminal Hackers Who Broke Into Its System.	12
2. The Stolen PII Is Not A “Consumer Report” Under The FCRA.	13
3. Because Plaintiffs’ § 1681b Claims Fail, Their § 1681e(a) Claim Necessarily Fails As Well	15
B. Plaintiffs’ Claims of Injury Globally Fail To Allege Cognizable Harms Caused By Equifax.....	16
1. Plaintiffs’ Non-Harms And Speculative Future Harms Are Not Legally Cognizable Injuries.....	16
2. Independently, Plaintiffs Have Failed To Allege That Equifax Proximately Caused Their Alleged Injuries.	20
3. Economic Loss Doctrine.....	23

C. Plaintiffs’ Negligence And Declaratory Judgment Claims Must Be Dismissed.	24
1. Georgia Law Does Not Impose Any Applicable Duty Of Care, So Plaintiffs’ Negligence And Declaratory Judgment Claims Must Be Dismissed.....	24
2. The FCRA Imposes No Relevant Duty Of Care.....	33
3. No Equifax Act Or Omission Proximately Caused Any Cognizable Injury To Plaintiffs.....	33
D. Plaintiffs’ Negligence <i>Per Se</i> Claim Must Be Dismissed	34
1. Plaintiffs Cannot Maintain A Negligence <i>Per Se</i> Action Under The Statutes They Cite.....	34
2. Plaintiffs Have Not Sufficiently Alleged Injury Or Proximate Causation	38
E. Plaintiffs’ Georgia Fair Business Practices Act Claim Must Be Dismissed.	38
1. <i>McConnell III</i> Confirms That The Georgia Fair Business Practices Act Does Not Require Safeguarding PII.....	38
2. Plaintiffs Have Not Pleaded Reliance.	39
3. No Plaintiff Has Alleged Injuries Caused By Any Misrepresentation.....	40
4. The GFBPA Forbids Class Actions	40
F. Plaintiffs’ Unjust Enrichment Claim Must Be Dismissed	41
II. THE CONTRACT AND FCRA DISCLOSURE CLAIMS MUST BE DISMISSED.....	43
A. Both Breach Of Contract Claims Must Be Dismissed.	43

1. The Privacy Policy Is Not A Contract, And Even If It Were It Does Not Impose The Duty Plaintiffs Assert	44
2. Plaintiffs Do Not Properly Allege Breach Of An Implied Contract.....	48
3. Plaintiffs Identify No Contractual Duty To “Promptly Alert Or Give Notice Of [A] Breach”	50
B. The FCRA Disclosure Plaintiffs’ Claims Must Be Dismissed	50
III. EACH PLAINTIFF’S CLAIMS UNDER HIS OR HER LOCAL STATE STATUTES MUST BE DISMISSED.	52
A. Plaintiffs’ Claims Under State Business Fraud And Consumer Protection Statutes Must Be Dismissed.	53
1. Foreign States’ Deceptive-Trade-Practices Laws Cannot Govern Conduct That Took Place In Georgia.....	53
2. Plaintiffs Have Failed To Plead Fraud With Particularity.	56
3. Plaintiffs Have Failed To Sufficiently Allege Scienter.....	59
4. Plaintiffs’ Allegations Of Injury Are Insufficiently Specific Or Substantial To Survive Dismissal.....	60
5. Plaintiffs’ Claims Under Statutes Requiring Consumer Transactions Must Be Dismissed.	61
6. Plaintiffs Allege No Facts Sufficient To Establish A Duty To Disclose.	62
7. Plaintiffs’ Claims for Damages Under Statutes Providing Only Equitable Relief Must Be Dismissed.....	63
8. Plaintiffs’ Claims Under Statutes Providing No Relevant Private Right Of Action Must Be Dismissed.....	64

9. Plaintiffs’ Claim Under The Georgia Uniform Deceptive Trade Practices Act Fails Because It Relies On A Duty Rejected In *McConnell III*.64

B. Plaintiffs’ Claims Under Data-Breach-Notification Statutes Must Be Dismissed.....65

1. Plaintiffs Have Alleged Claims Under Statutes That Do Not Provide A Private Right Of Action.65

2. Plaintiffs Have Failed To Allege A Violation Of Any State Data Breach Statute.....66

3. Plaintiffs Have Failed To Allege A Violation Of The Maryland Social Security Number Privacy Act.68

4. Plaintiffs Have Failed To Allege Any Injury Resulting From Any Delay In Notification.68

C. Plaintiffs Cannot Maintain Claims For Nonexistent Plaintiffs.....69

D. Plaintiffs’ O.C.G.A. § 13-6-11 Claim Should Be Dismissed.69

CONCLUSION.....70

TABLE OF AUTHORITIES

Cases

<i>Access Mgmt. Grp. L.P. v. Hanham</i> , 812 S.E.2d 509 (Ga. Ct. App. 2018)	24
<i>Albany Urology Clinic, P.C. v. Cleveland</i> , 528 S.E.2d 777 (Ga. 2000)	28
<i>Alexander v. Sandoval</i> , 532 U.S. 275 (2001)	36
<i>Ali v. Vikar Mgmt. Ltd.</i> , 994 F. Supp. 492 (S.D.N.Y. 1998)	14
<i>Am. Dental Ass’n v. Cigna Corp.</i> , 605 F.3d 1283 (11th Cir. 2010)	57
<i>Ambrosia Coal & Constr. Co. v. Pages Morales</i> , 482 F.3d 1309 (11th Cir. 2007)	10
<i>Andrews v. Kinsel</i> , 40 S.E. 300 (Ga. 1901)	22, 23
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	10, 59
<i>Baldwin v. Hosp. Auth. of Fulton Cty.</i> , 383 S.E.2d 154 (Ga. Ct. App. 1989)	30
<i>Bellsouth Telecommc’ns LLC v. Cobb Cty.</i> , 802 S.E.2d 686 (Ga. Ct. App. 2017)	34
<i>Bickley v. Dish Network, LLC</i> , 751 F.3d 724 (6th Cir. 2014)	14
<i>BMW of N. Am., Inc. v. Gore</i> , 517 U.S. 559 (1996)	55
<i>Bonaparte v. Tax Ct.</i> , 104 U.S. 592 (1881)	55
<i>Bradford v. WR Starkey Mortg., LLP</i> , No. 2:06-CV-86-WCO 2006 WL 8436036 (N.D. Ga. Nov. 17, 2006)	44

<i>Bradley Center, Inc. v. Wessner</i> , 296 S.E.2d 693 (Ga. 1982)	30
<i>Bravo v. United States</i> , 577 F.3d 1324 (11th Cir. 2009)	27
<i>Brock v. Avery Co.</i> , 110 S.E.2d 122 (Ga. Ct. App. 1959)	34, 35, 37
<i>Broughton v. Johnson</i> , 545 S.E.2d 370 (Ga. Ct. App. 2001)	45, 46
<i>Burnett v. Stagner Hotel Courts, Inc.</i> , 821 F. Supp. 678 (N.D. Ga. 1993)	49
<i>Burton v. MAPCO Express, Inc.</i> , 47 F. Supp. 3d 1278 (N.D. Ala. 2014)	20
<i>Cahlin v. Gen. Motors Acceptance Corp.</i> , 936 F.2d 1151 (11th Cir. 1991)	16
<i>Campbell v. Albers</i> , 39 N.E.2d 672 (Ill. App. Ct. 1942)	54
<i>Carmax Auto Superstores, Inc. v. Sibley</i> , 194 F. Supp. 3d 392 (D. Md. 2016)	65
<i>Channing v. Equifax, Inc.</i> , No. 5:11-CV-293-FL, 2013 WL 593942 (E.D.N.C. Feb. 15, 2013)	13
<i>Clark v. Aaron's, Inc.</i> , 914 F. Supp. 2d 1301 (N.D. Ga. 2012)	42
<i>Clinton v. City of New York</i> , 524 U.S. 417 (1998)	52
<i>Comm. Bank of Trenton v. Schnuck Mkts., Inc.</i> , 887 F.3d 803 (7th Cir. 2018)	29, 31
<i>Coon v. Med. Ctr., Inc.</i> , 797 S.E.2d 828 (Ga. 2017)	11
<i>Crespo v. Coldwell Banker Mortg.</i> , 599 F. App'x 868 (11th Cir. 2014)	56

<i>CSX Transp., Inc. v. Williams</i> , 608 S.E.2d 208 (Ga. 2005)	28
<i>Cumberland Contractors, Inc. v. State Bank & Trust Co.</i> , 755 S.E.2d 511 (Ga. Ct. App. 2014)	17
<i>David G. Brown, P.E., Inc. v. Kent</i> , 561 S.E.2d 89 (Ga. 2002)	70
<i>De Bouse v. Bayer AG</i> , 922 N.E.2d 309 (Ill. 2009).....	58
<i>Dolmage v. Combined Ins. Co. of Am.</i> , No. 14 C 3809, 2015 WL 292947 (N.D. Ill. Jan. 21, 2015)	13
<i>Donaldson v. Olympic Health Spa, Inc.</i> , 333 S.E.2d 98 (Ga. Ct. App. 1985)	48
<i>Dotzler v. Perot</i> , 914 F. Supp. 328 (E.D. Mo. 1996), <i>aff'd</i> 124 F.3d 207 (8th Cir. 1997)	14
<i>Dowis v. Mud Slingers, Inc.</i> , 621 S.E.2d 413 (Ga. 2005)	11
<i>Driebe v. Cox</i> , 416 S.E.2d 314 (Ga. Ct. App. 1992)	30
<i>Dyer v. Nw. Airlines Corps.</i> , 334 F. Supp. 2d 1196 (D.N.D. 2004)	46
<i>Ekeledo v. Amporful</i> , 642 S.E.2d 20 (Ga. 2007)	44, 48
<i>Ermutlu v. McCorkle</i> , 416 S.E.2d 792 (Ga. Ct. App. 1992)	30
<i>Farmer v. Phillips Agency, Inc.</i> , 285 F.R.D. 688 (N.D. Ga. 2012)	15
<i>Fejzulai v. Sam's West, Inc.</i> , 205 F. Supp. 3d 723 (D.S.C. 2016)	41
<i>Finnerty v. State Bank & Trust Co.</i> , 687 S.E.2d 842 (Ga. Ct. App. 2009)	17, 18

<i>Flatirons Bank v. Alan W. Steinberg Ltd. P’ship</i> , 233 So. 3d 1207 (Fla. 3d DCA 2017).....	54
<i>Fulton v. Hecht</i> , 580 F.2d 1243 (5th Cir. 1978).....	36
<i>Galaria v. Nationwide Mut. Ins. Co.</i> , No. 2:13-cv-118, 2017 WL 4987663 (S.D. Ohio Aug. 16, 2017).....	13
<i>General Electric Co. v. Lowe’s Home Centers, Inc.</i> , 608 S.E.2d 636 (Ga. 2005).....	23, 28
<i>Goldstein, Garber & Salama, LLC v. J.B.</i> , 797 S.E.2d 87 (Ga. 2017).....	22
<i>Grange Mut. Cas. Co. v. Woodard</i> , 797 S.E.2d 814 (Ga. 2017).....	48
<i>Griffin v. Dugger</i> , 823 F.2d 1476 (11th Cir. 1987).....	16, 69
<i>Grupo Televisa, S.A. v. Telemundo Commc’ns Grp., Inc.</i> , 485 F.3d 1233 (11th Cir. 2007).....	11
<i>Healy v. Beer Inst.</i> , 491 U.S. 324 (1989).....	55
<i>Hines v. MidFirst Bank</i> , No. 1:12-cv-2527-TWT, 2013 WL 609401 (N.D. Ga. Jan. 8, 2013) (Rpt. & Rec.), <i>adopted</i> 2013 WL 603883 (N.D. Ga. Feb. 19, 2013).....	56
<i>Hite v. Anderson</i> , 643 S.E.2d 550 (Ga. Ct. App. 2007).....	38
<i>Houston v. Bedgood</i> , 588 S.E.2d 437 (Ga. Ct. App. 2003).....	30
<i>Huggins v. Aetna Cas. & Sur. Co.</i> , 264 S.E.2d 191 (Ga. 1980).....	32
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016).....	46

<i>In re Arby's Rest. Grp. Inc. Litig.</i> , No. 1:17-cv-0514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018).....	29, 31, 36
<i>In re Experian Data Breach Litig.</i> , No. SACV 15-1592 AG (DFMx), 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)	13, 16, 61
<i>In re Home Depot Customer Data Security Breach Litig.</i> , No. 14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016)	29, 30, 36
<i>In re New Motor Vehicles Canadian Exp. Antitrust Litig.</i> , 241 F.R.D. 77 (D. Me. 2007)	40, 41
<i>In re Nw. Airlines Privacy Litig.</i> , No. Civ. 04-126 (PAM/JSM), 2004 WL 1278459 (D. Minn. June 6, 2004)	46
<i>In re Sony Gaming Networks & Customer Data Breach Litig.</i> , 903 F. Supp. 2d 942 (S.D. Cal. 2012)	58, 60
<i>In re Stand 'n Seal Prods. Liab. Litig.</i> , No. 1:07-MD-1804-TWT, 2009 WL 2998003 (N.D. Ga. Sept. 15, 2009)	11
<i>In re SuperValu, Inc.</i> , 870 F.3d 763 (8th Cir. 2017).....	18, 19, 22, 60
<i>In re VTech Data Breach Litig.</i> , No. 15-CV-10889, 2018 WL 1863953 (N.D. Ill. Apr. 18, 2018)	48
<i>In re Zappos.com, Inc.</i> , 2013 WL 4830497 (D. Nev. 2013).....	64
<i>Infrasource, Inc. v. Hahn Yalena Corp.</i> , 613 S.E.2d 144 (Ga. Ct. App. 2005)	63
<i>Katz v. Pershing</i> , 806 F. Supp. 2d 452 (D. Mass. 2011).....	64
<i>KMS Rest. Corp. v. Wendy's Int'l, Inc.</i> , 361 F.3d 1321 (11th Cir. 2004)	27

<i>LabMD v. Fed. Trade Comm’n</i> , No. 16-16270, — F.3d —, 2018 WL 3056794 (11th Cir. June 6, 2018)	35, 36
<i>Legacy Acad., Inc. v. Mamilove, LLC</i> , 761 S.E.2d 880 (Ga. Ct. App. 2014)	36
<i>Lisk v. Lumber One Wood Preserving, LLC</i> , 792 F.3d 1331 (11th Cir. 2015)	41
<i>McConnell v. Dep’t of Labor (McConnell I)</i> , 787 S.E.2d 794 (Ga. Ct. App. 2016)	25
<i>McConnell v. Dep’t of Labor (McConnell II)</i> , 805 S.E.2d 79 (Ga. 2017)	25
<i>McConnell v. Ga. Dep’t of Labor (McConnell III)</i> , No. A16A0655, — S.E.2d. —, 2018 WL 2173252 (Ga. Ct. App. May 11, 2018)	passim
<i>McDonald v. Equifax Inc.</i> , No. 3:15-CV-3212-B, 2017 WL 879224 (N.D. Tex. Mar. 6, 2017)	13
<i>Miller v. Experian Info. Sols. Inc.</i> , No. 3:13-cv-090, 2015 WL 728342 (S.D. Ohio Feb. 19, 2015)	51
<i>Miller v. Trans Union, LLC</i> , 644 F. App’x 444 (6th Cir. 2016)	51
<i>Miranda v. Fulton DeKalb Hosp. Auth.</i> , 644 S.E.2d 164 (Ga. Ct. App. 2007)	30
<i>Morris v. Baxter</i> , 483 S.E.2d 650 (Ga. Ct. App. 1997)	20, 21
<i>Next Century Commc’ns Corp. v. Ellis</i> , 318 F.3d 1023 (11th Cir. 2003)	58
<i>Norman v. Jones Lang Lasalle Ams., Inc.</i> , 627 S.E.2d 382 (Ga. Ct. App. 2006)	34, 37

<i>Parker v. Equifax Info. Servs., LLC</i> , No. 2:15-cv-14365, 2017 WL 4003437 (E.D. Mich. Sep. 12, 2017)	14
<i>Pate v. Oakwood Mobile Homes, Inc.</i> , 374 F.3d 1081 (11th Cir. 2004)	32
<i>Perez v. Mortg. Bankers Ass’n</i> , 135 S.Ct. 1199 (2015)	37
<i>Pisciotta v. Old Nat’l Bancorp.</i> , 499 F.3d 629 (7th Cir. 2007)	17
<i>Planned Parenthood v. Nixon</i> , 220 S.W.3d 732 (Mo. 2007) (en banc)	54
<i>Provost v. Aptos, Inc.</i> , No. 1:17-cv-02120-ELR, 2018 WL 1465766 (N.D. Ga. Mar. 12, 2018)	20
<i>Pub. Citizen v. U.S. Dep’t of Justice</i> , 491 U.S. 440 (1989)	52, 55
<i>Purcell v. Breese</i> , 552 S.E.2d 865 (Ga. Ct. App. 2001)	30
<i>Randolph v. ING Life Ins. & Annuity Co.</i> , 973 A.2d 702 (D.C. 2009)	18, 19
<i>Reinbrecht v. Walgreen Co.</i> , 742 N.W.2d 243 (Neb. Ct. App. 2007)	63
<i>Remax Mountain Co. v. Tabsum, Inc.</i> , 634 S.E.2d 77 (Ga. Ct. App. 2006)	23
<i>Rite Aid of Ga., Inc. v. Peacock</i> , 726 S.E.2d 577 (Ga. Ct. App. 2012)	17
<i>Rodi v. S. New England School of Law</i> , 532 F.3d 11 (1st Cir. 2008)	58
<i>Sawyer v. Market Am., Inc.</i> , 661 S.E.2d 750 (N.C. Ct. App. 2008)	54
<i>Sitterli v. Csachi</i> , 811 S.E.2d 454 (Ga. Ct. App. 2018)	41, 42, 43

<i>Smith v. Waverly Partners, LLC</i> , No. 3:10-CV-28, 2011 WL 3564427 (W.D.N.C. Aug. 12, 2011)	14
<i>State Farm Mut. Auto Ins. Co. v. Hernandez Auto Painting & Body Works, Inc.</i> , 719 S.E.2d 597 (Ga. Ct. App. 2011)	65
<i>State Farm v. Campbell</i> , 538 U.S. 408 (2003)	54, 56
<i>Stires v. Carnival Corp.</i> , 243 F. Supp. 2d 1313 (M.D. Fla. 2002)	56
<i>Sun Oil Co. v. Wortman</i> , 486 U.S. 717 (1988)	55
<i>Tiismann v. Linda Martin Homes Corp.</i> , 637 S.E.2d 14 (Ga. 2006)	39
<i>Torres v. Wendy's Co.</i> , 195 F. Supp. 3d 1278 (M.D. Fla. 2016)	19, 20, 60
<i>Torres v. Wendy's Int'l LLC</i> , No. 6:16-cv-210-Orl-40DCI, 2017 WL 8780453 (M.D. Fla. Mar. 21, 2017)	65
<i>Trans Union Corp. v. FTC</i> , 81 F.3d 228 (D.C. Cir. 1996)	15
<i>W. Union Tel. Co. v. Epley</i> , 218 S.W. 528 (Tex. Civ. App. 1920)	54
<i>Walton v. UCC X, Inc.</i> , 640 S.E.2d 325 (Ga. Ct. App. 2006)	30
<i>Ward v. United Airlines</i> , 889 F.3d 1068 (9th Cir. 2018)	54
<i>Washington v. CSC Credit Servs.</i> , 199 F.3d 263 (5th Cir. 2000)	15
<i>Weathers v. Dieniahmar Music, LLC</i> , 788 S.E.2d 852 (Ga. Ct. App. 2016)	45
<i>Wells Fargo Bank, N.A. v. Jenkins</i> , 744 S.E.2d 686 (Ga. 2013)	passim

<i>Willingham v. Global Payments, Inc.</i> , No. 1:12-cv-01157-RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013).....	23, 32, 40
<i>Wilson v. Clark Atlanta Univ., Inc.</i> , 794 S.E.2d 422 (Ga. Ct. App. 2016)	45
<i>Wis. Indus. Energy Grp., Inc. v. Pub. Serv. Comm’n</i> , 819 N.W.2d 240 (Wis. 2012)	54

Statutes

10 Me. Rev. Stat. § 1213.....	63
15 U.S.C. § 1681	12
15 U.S.C. § 1681a	14
15 U.S.C. § 1681g.....	50, 51
15 U.S.C. § 45.....	34, 35
18 U.S.C. § 1028.....	23
18 U.S.C. § 1030	21
6 Del. Code Ann. § 12B-102	67
6 Del. Code Ann. 12b-104	65
815 Ill. Comp. Stat. § 510/3	63
C.G.S.A. § 36a-701b.....	67
Cal. Civ. Code § 1798.84.....	68
Colo Rev. Stat § 6-1-716	65
Iowa Code § 715C.2.....	65
Kan. Stat. Ann. § 50-7a02.....	65
Mass. Gen. Laws 93A § 4.....	64
Mass. Gen. Laws 93H § 6	64
Md. Comm. Code § 14-3402	68
Md. Comm. Code § 14-3504	67
Mich. Comp. Laws Ann. § 445.72.....	65

Minn. Stat § 325D.45	63
Mont. Code Ann. § 30-14-1705	65
N.J. Stat. § 56:8-163	65
N.R.S. §§ 598.0983–0989	64
N.Y. Gen. Bus. Law § 349	54
N.Y. Gen. Bus. Law § 899-aa	65
Neb. Rev. Stat. § 87-303	63
O.C.G.A. § 10-1-399	40
O.C.G.A. § 51-12-8	20
O.C.G.A. § 9-2-7	42, 43
Tenn. Code Ann. § 47-18-2107	67
Wash. Rev. Code § 19.255.010	67
Wis. Stat. § 134.98	67
Wyo. Stat. Ann. § 40-12-502	65

Rules

16 C.F.R. § 436.2	37
16 C.F.R. Part 600	15
Fed. R. Civ. P. 9	10, 57

Treatises

Restatement (Second) of Torts § 323	32
Restatement (Second) of Torts § 324A	32

INTRODUCTION

Defendants Equifax Inc. (“Equifax”), its consumer-reporting-agency subsidiary Equifax Information Services LLC (“EIS”), and its consumer-services subsidiary Equifax Consumer Services LLC (“ECS”) are committed to safeguarding consumers’ personally identifying information (“PII”). They have built a strong security infrastructure to protect the information they receive, maintain, and send. Nevertheless, in 2017, criminal hackers invaded Equifax’s systems and stole records containing the PII of over 145 million U.S. consumers.

Upon discovering the breach, Equifax took quick action to stop the intrusion, further shore up its systems’ defenses, and diligently investigate the nature and scope of the intrusion. Once Equifax identified substantially all of the affected consumers, it promptly announced its findings and took the unprecedented step of offering a robust package of consumer services, free of charge, to *all* U.S. consumers—whether their PII had been stolen or not.

Plaintiffs, on behalf of a putative nationwide class and numerous putative subclasses of consumers, allege that criminals stole their PII in the attack. They assert 99 claims for relief in a 556-page Consolidated Consumer Class Action Complaint (“CCC”). But while the CCC is long on words, it is short on operative facts, particularly regarding the named Plaintiffs. Plaintiffs’ grab-bag approach to

pleading underscores that none of the causes of action they have asserted fits the facts of this case or entitles them to relief. To the contrary, the CCC suffers from numerous irreparable defects, highlighting that a class action lawsuit is an inappropriate vehicle for addressing consumers' highly individualized concerns over the theft of PII.

First, Plaintiffs' claims under the federal Fair Credit Reporting Act ("FCRA") categorically fail. The FCRA regulates, among other things, how consumer reporting agencies ("CRAs") like EIS are permitted to "furnish" credit reporting data. It does not apply when data unassociated with creditworthiness is stolen from—not "furnished" by—a CRA or its affiliates.

Second, Plaintiffs fail to allege facts showing that they have suffered a legally sufficient injury as a result of the data breach. Most Plaintiffs merely allege that their PII was disclosed to third parties, but that is not itself a legally cognizable harm. Nor are the vague and speculative future harms that Plaintiffs allege.

And even assuming some Plaintiffs have pleaded a sufficient injury, no Plaintiff has plausibly alleged that the injury was caused by the *Equifax* data breach. Data breaches today are commonplace—there were more than 1,500 breaches in 2017 alone—and no Plaintiff pleads that his or her PII was *not* stolen in any prior breach. It is, therefore, entirely speculative for any Plaintiff to

attribute any alleged fraud or identity theft to the Equifax data breach, as opposed to another breach or fraudulent act. Further, even if a Plaintiff could somehow trace any alleged injury to the Equifax data breach (and no Plaintiff has alleged facts that would permit this Court to do so), those claims would still fail because a chain of criminal acts by unknown third parties broke any causal connection between Equifax's conduct and the purported injury.

Plaintiffs' inability to plead that they suffered a legally sufficient harm—or that the Equifax data breach caused any alleged harm—permeates the CCC, requiring dismissal of the lion's share of Plaintiffs' claims.

Third, Plaintiffs' negligence and negligence *per se* claims fail because they are premised on a duty of care that does not exist under applicable statutory or common law. Plaintiffs allege that their negligence claims are governed by Georgia law, and in May 2018, the Georgia Court of Appeals issued a well-reasoned decision holding that *no duty of care to safeguard another's PII exists in Georgia*.¹ That decision binds this Court.

Fourth, Plaintiffs' claims under the Georgia Fair Business Practices Act fail because the statute does not impose a duty to safeguard consumers' PII. The

¹ *McConnell v. Ga. Dep't of Labor*, — S.E.2d. —, No. A16A0655, 2018 WL 2173252 (Ga. Ct. App. May 11, 2018) (“*McConnell III*”), *cert. pending*.

claims also fail because Plaintiffs have not pleaded that they gave their PII to Equifax in *reliance* on any misrepresentation—on the contrary, Plaintiffs affirmatively allege that they did *not* provide their PII to Equifax.

Fifth, Plaintiffs’ unjust enrichment claim lacks merit. To state such a claim, Plaintiffs would have to allege that they conferred their PII as a valuable benefit on Equifax and reasonably expected to be repaid. But Plaintiffs expressly allege *either* that they did not give their PII to Equifax *or* that they had contracts with Equifax. Either way, they cannot state a claim for unjust enrichment.

Sixth, although a subset of Plaintiffs assert claims for breach of contract, they rely entirely on language in Equifax’s Privacy Policy that was *not* made part of any contract these Plaintiffs had with Equifax.

Seventh, Plaintiffs raise a host of claims under various state consumer-protection and data-breach-notification statutes. But the consumer-protection statutes on which Plaintiffs rely cannot govern conduct that took place entirely in Georgia and that affected Plaintiffs, if at all, only indirectly through the criminal acts of third parties. Constitutional and statutory limits on the extraterritorial enforcement of state statutes place Equifax’s Georgia conduct beyond the power of other states to regulate. And even if these statutes did apply, Plaintiffs’ pleadings are defective. Their claims allege fraudulent misrepresentations, but were not

pleaded with the requisite particularity. Nor do Plaintiffs adequately plead either injury from any alleged misrepresentation or that they engaged in any consumer transactions with Equifax. Likewise, Plaintiffs assert defective claims under statutes that prohibit private plaintiffs from suing; fail to allege facts showing that Equifax unduly delayed notifying consumers about the data breach; and allege no facts showing that they were injured by any delay in notification.

Equifax shares Plaintiffs' concerns about the safety and security of consumers' PII—and has taken historic strides to strengthen its cybersecurity practices following the breach. But the CCC is no solution to Plaintiffs' concerns. Its claims are defective as a matter of law and must be dismissed.

FACTUAL BACKGROUND & PROCEDURAL HISTORY

A. The parties. Plaintiffs are 96 consumers, allegedly representing consumers in all fifty U.S. states plus the District of Columbia,² who claim that their PII was compromised when malicious hackers infiltrated Equifax's computer systems between May 13 and July 30, 2017. *See* CCC ¶¶ 13–108. Although they banded together to file a purported class action lawsuit, Plaintiffs allege highly disparate claims and harms arising from the theft of their PII.

² Although Plaintiffs allege claims under the laws of Puerto Rico and the Virgin Islands, no Plaintiff alleges any connection to either of those territories. *See generally* CCC ¶¶ 13–108.

Defendant Equifax, a Georgia corporation with its principal place of business in Atlanta, Georgia, is a leading global provider of information, human-resources, and data-analytics services for businesses, governments, and consumers. Information stored on Equifax servers was accessed during the 2017 data breach.

Defendant EIS, a subsidiary of Equifax, is a Georgia limited liability company. EIS is a national consumer reporting agency that stores and furnishes consumer credit reporting data. EIS records were *not* accessed during the data breach. *See* CCC ¶ 272.

Defendant ECS, a subsidiary of Equifax, is a Georgia limited liability company that (among other things) offers credit monitoring services to consumers.

B. The Equifax Data Breach.³ Late in the evening of July 29, 2017, Equifax Security personnel observed suspicious network traffic associated with its U.S. online dispute portal web application. *See* CCC ¶ 196. Equifax Security promptly investigated and blocked this suspicious traffic, and continued monitoring network traffic associated with the portal. *See id.* ¶ 197. The next day, Equifax Security identified further suspicious activity and took the dispute portal offline. *See id.*

³ For purposes of this Motion to Dismiss, Equifax accepts, as it must, the factual allegations in the CCC as true.

Equifax then promptly retained Mandiant, a leading independent cybersecurity firm, to assist in a comprehensive forensic review. *See* CCC ¶ 201. Equifax also reported the incident to the FBI. *See id.*

Equifax and Mandiant diligently analyzed forensic traces in Equifax's systems to assess the scope of the intrusion. *See, e.g.,* CCC ¶¶ 202, 204, 206, 207, 212. Investigation revealed that hackers had exploited a vulnerability in Apache Struts, an open-source programming framework, to break into the dispute portal. *See id.* ¶ 246. As the investigation proceeded, Equifax learned that the attackers might have accessed database tables containing consumers' PII. *See id.* ¶ 206. But neither Equifax nor Mandiant found any evidence of unauthorized activity in EIS's core consumer or commercial credit-reporting databases. *See id.* ¶ 272. Equifax eventually determined that, between May 13 and July 30, 2017, the criminal hackers had accessed certain files containing PII. *See id.* ¶ 195.

Despite those prompt and diligent efforts, the size and complexity of the intrusion meant that determining its scope—and identifying the consumers whose PII had been affected—required several weeks. *See* CCC ¶¶ 212. By September 4, 2017, Equifax had identified 143 million consumers whose PII had been accessed. *See id.* Ultimately, Equifax determined that the attackers had accessed 146.6 million U.S. consumers' names and birthdates, 145.5 million Social Security

numbers, 99 million addresses, 20.3 million telephone numbers, and 17.6 million driver's license numbers. *See id.* ¶¶ 212 & 257. The attackers also accessed much smaller amounts of other data—1.8 million email addresses, 209,000 payment card credentials, 97,500 tax IDs, and 27,000 driver's license state fields. *See id.*

C. Equifax's Notification and Remediation Efforts. On September 7, 2017, once it had determined the identities of the consumers whose PII was potentially affected in the data security breach, Equifax issued a national press release announcing the incident. *See CCC* ¶ 227. It also provided written notification of the incident to all state attorneys general and to state and federal regulatory bodies, including the Federal Trade Commission ("FTC"). Equifax established a dedicated call center to answer consumers' questions. *See id.* ¶ 149. And it set up a dedicated website providing a lookup tool to tell consumers whether their PII was compromised in the breach, along with more information about the incident and a list of state specific data breach disclosures. *See id.* ¶¶ 231–32. Equifax also directly notified by mail consumers whose payment-card information or dispute documents had been accessed. *See, e.g., CCC* ¶¶ 26, 33 & 60.

In an unprecedented step to help consumers protect their PII following the breach, Equifax offered *all* U.S. consumers a full suite of credit-monitoring and identity-theft-protection services free of charge, regardless of whether their PII had

been compromised in the breach. *See* CCC ¶ 233. Those services include 3-bureau credit monitoring, free Equifax credit reports, the ability to lock and unlock Equifax credit reports, identity-theft insurance, and internet scanning for Social Security numbers. Millions of consumers registered for these free services. Equifax also offered free credit freezes (and refunds for previously implemented freezes) to *all* U.S. consumers. And starting in January 2018, Equifax rolled out its Lock & Alert service, which enables all U.S. consumers to easily lock and unlock their Equifax credit reports for free, for life using a computer or smartphone.

D. Procedural Background. On September 7, 2017—the very day Equifax announced the data breach—plaintiffs began filing lawsuits throughout the country. After consolidation of hundreds of cases in this Court and appointment of lead counsel, Plaintiffs filed their 556-page CCC. The CCC asserts six claims on behalf of a putative nationwide class of all U.S. consumers whose PII was compromised in the data breach: (i) violation of the FCRA; (ii) negligence; (iii) negligence *per se*; (iv) violation of Georgia’s Fair Business Practices Act; (v) unjust enrichment; and (vi) declaratory judgment. The CCC further asserts breach-of-contract claims on behalf of putative “Contract Subclasses” consisting of affected U.S. consumers who either bought Equifax’s credit-monitoring or identity-theft-protection services, or (allegedly subject to the Company’s Privacy

Policy) gave PII to Equifax as part of some other transaction. The CCC also asserts a claim under section 1681(g) of the FCRA on behalf of a putative subclass of affected U.S. consumers who obtained credit-file disclosures from Equifax between July 29, 2017 and the present. Finally, the CCC asserts a host of claims under various state consumer-fraud and deceptive-trade-practices laws, and data-breach-notification statutes, on behalf of various putative Statewide Subclasses.

LEGAL STANDARD & CHOICE OF LAW

A. Pleading requirements.

To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain “sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotation marks omitted). The standard “demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation”; mere “labels and conclusions” or a “formulaic recitation of the elements of a cause of action will not do.” *Id.* (quotation marks omitted). The standard is higher for claims sounding in fraud. Those claims require the plaintiff to plead “with particularity,” Fed. R. Civ. P. 9(b), which requires detailed allegations of the circumstances surrounding the alleged fraud or misrepresentation. *See Ambrosia Coal & Constr. Co. v. Pages Morales*, 482 F.3d 1309, 1316–17 (11th Cir. 2007).

B. Choice of law.

“A federal court sitting in diversity will apply the conflict-of-laws rules of the forum state.” *Grupo Televisa, S.A. v. Telemundo Commc’ns Grp., Inc.*, 485 F.3d 1233, 1240 (11th Cir. 2007). Georgia’s choice-of-law rule is *lex loci delicti*—the law of the place of injury. *Dowis v. Mud Slingers, Inc.*, 621 S.E.2d 413, 419 (Ga. 2005). As a result, when *statutes* of a foreign state govern a claim sounding in tort, Georgia courts defer “[a]s a matter of comity” to those statutes unless they are inconsistent with Georgia’s public policy. *Coon v. Med. Ctr., Inc.*, 797 S.E.2d 828, 834 (Ga. 2017). But when no statute governs the claim, “a Georgia court will apply the common law as expounded by the courts of Georgia.” *Id.*

Plaintiffs have identified no foreign-state statutes that govern their common-law claims, and instead assert that “the common law of Georgia applies to the nationwide common law claims of all Nationwide Class members.” CCC ¶ 313. For the purposes of this Motion to Dismiss, therefore, this Court should presume that Georgia common law governs those claims. *In re Stand ’n Seal Prods. Liab. Litig.*, No. 1:07-MD-1804-TWT, 2009 WL 2998003, at *2 (N.D. Ga. Sept. 15, 2009) (“If the parties do not identify any foreign statutes in their pleadings, it is presumed that no foreign statutes are involved.”).

ARGUMENT

I. THE CLAIMS PLAINTIFFS ASSERT ON BEHALF OF A PUTATIVE NATIONWIDE CLASS ARE DEFECTIVE AND MUST BE DISMISSED.

A. Plaintiffs' Fair Credit Reporting Act Claims Must Be Dismissed.

All Plaintiffs, on behalf of a putative nationwide class, have asserted a claim for violation of the FCRA, 15 U.S.C. § 1681 *et seq.* They allege that Equifax “furnished Plaintiffs’ ... consumer reports to unauthorized third parties” in violation of § 1681b, and that Equifax “failed to maintain reasonable procedures designed to limit” to permissible purposes “the furnishing of Class members’ consumer reports,” in violation of § 1681e. CCC ¶¶ 321, 324 & 326. But under § 1681b, Equifax did not “furnish” information to the criminal hackers, and in any event, the stolen PII was not a “consumer report.” And because Plaintiffs cannot show a violation of § 1681b, the § 1681e claim fails.

1. Equifax Did Not “Furnish” Any Information To The Criminal Hackers Who Broke Into Its System.

Plaintiffs cannot maintain a claim under § 1681b because Equifax did not “furnish” information to the criminals who hacked into its systems. To the contrary, the attackers *stole* information *from* Equifax. Under the FCRA, “furnishing” requires a purposeful disclosure. Courts have unanimously ruled that information stolen from a CRA is not information the CRA “furnished.” *E.g.*,

Galaria v. Nationwide Mut. Ins. Co., No. 2:13-cv-118, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017) (data obtained from data breach was stolen, not “furnished”); *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMx), 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016) (“[T]hese allegations are all based on the fact that Defendants’ data was *stolen* by a third party, not furnished to the third party.”); *see also Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *4 (N.D. Ill. Jan. 21, 2015) (collecting cases). Even assuming all Defendants were CRAs subject to the FCRA (and only EIS is actually a CRA⁴), Plaintiffs’ failure to allege that Equifax “furnish[ed]” *anything* to criminal hackers requires dismissal of the § 1681b claim.

2. The Stolen PII Is Not A “Consumer Report” Under The FCRA.

Plaintiffs’ FCRA claims must be dismissed for a second independent reason. The information compromised in the data breach consists of names, birthdates, Social Security numbers, physical and email addresses, gender identifiers, telephone numbers, payment card numbers and expiry dates, tax IDs, driver’s license numbers, and driver’s license state of issuance data. *See CCC* ¶ 257. As a matter of law, none of this PII in itself “bear[s] on” consumers’ creditworthiness,

⁴ *See, e.g., McDonald v. Equifax Inc.*, No. 3:15-CV-3212-B, 2017 WL 879224, at *8 (N.D. Tex. Mar. 6, 2017).

character, or “mode of living.” *See* 15 U.S.C. § 1681a(d)(1) (defining “consumer report”). Courts have therefore consistently ruled that this type of information, known as “header” data, does not constitute a “consumer report” under the FCRA. *See id.*; *Bickley v. Dish Network, LLC*, 751 F.3d 724, 729 (6th Cir. 2014) (“header information” was not a “consumer report”); *Parker v. Equifax Info. Servs., LLC*, No. 2:15-cv-14365, 2017 WL 4003437, at *1, *3 (E.D. Mich. Sept. 12, 2017) (“header data” including “name, phone number, social security number, date of birth, driver’s license, current address, and time spent at that address” “does not constitute a consumer report because the information does not bear on ... credit worthiness”); *Smith v. Waverly Partners, LLC*, No. 3:10-CV-28, 2011 WL 3564427, at *5 (W.D.N.C. Aug. 12, 2011) (plaintiff’s “name, Social Security Number, prior addresses, date of birth, and driver’s license information” was “not a consumer report”); *Ali v. Vikar Mgmt. Ltd.*, 994 F. Supp. 492, 499 (S.D.N.Y. 1998) (“address information” was not a “consumer report”); *Dotzler v. Perot*, 914 F. Supp. 328, 330–31 (E.D. Mo. 1996) (“address update containing plaintiffs’ names and current and former addresses as well as ... social security information” was not a “consumer report”), *aff’d*, 124 F.3d 207 (8th Cir. 1997).

The Federal Trade Commission—which has regulated CRAs for the past 40 years—agrees. In its 1995 Commentary on the FCRA, the FTC stated that “[a]

report limited solely to the consumer's name and address alone ... does not constitute a 'consumer report,' if it does not bear on" creditworthiness. Commentary on the FCRA, 16 C.F.R. Part 600 App. at 379–80 (1995); *see also Trans Union Corp. v. FTC*, 81 F.3d 228, 232 (D.C. Cir. 1996) (agreeing with the FTC that "lists from [a CRA's] credit reporting database based on such 'identifying information' as name, zip code, age, social security number or 'substantially similar identifiers'" were not "consumer report[s]"). Because the compromised PII does not "bear[] on" the statutory creditworthiness factors, it does not constitute a "consumer report," and Plaintiffs' § 1681b claim fails.

3. Because Plaintiffs' § 1681b Claims Fail, Their § 1681e(a) Claim Necessarily Fails As Well.

Plaintiffs' § 1681e claims fail for the same reasons. Section 1681e requires that "[e]very consumer reporting agency shall maintain reasonable procedures designed to ... limit the *furnishing of consumer reports* to the purposes listed under section 1681b of this title." (Emphasis added.) "[A] plaintiff bringing a claim that a reporting agency violated the 'reasonable procedures' requirement of § 1681e must first show that the reporting agency released the report in violation of § 1681b." *Washington v. CSC Credit Servs.*, 199 F.3d 263, 266–67 (5th Cir. 2000); *Farmer v. Phillips Agency, Inc.*, 285 F.R.D. 688, 698 (N.D. Ga. 2012) ("To sustain a claim under § 1681e(b), a consumer must show that an inaccurate report

was furnished by a CRA”); *see also Cahlin v. Gen. Motors Acceptance Corp.*, 936 F.2d 1151, 1156 (11th Cir. 1991) (same); *Experian*, 2016 WL 7973595, at *2 (plaintiff bringing a claim under § 1681e “must first show that the reporting agency released the report in violation of § 1681b”) (quotation marks omitted). Because Plaintiffs’ claims under § 1681b fail, Plaintiffs cannot maintain a claim under § 1681e(a).

B. Plaintiffs’ Claims of Injury Globally Fail To Allege Cognizable Harms Caused By Equifax.

All of Plaintiffs’ tort claims—including the claims for negligence, negligence *per se*, and state consumer-fraud-act violations—require a showing of injury and proximate causation. But Plaintiffs’ alleged injuries are not *legally cognizable harms*. And even if a Plaintiff has arguably alleged an injury, not one has alleged that Equifax proximately caused the injury. The failure to plead legally cognizable harms proximately caused by Equifax means that each claim for which injury and proximate causation are necessary elements must fail.

1. Plaintiffs’ Non-Harms And Speculative Future Harms Are Not Legally Cognizable Injuries.

Whether a given Plaintiff has alleged a cognizable injury is necessarily a highly individualized question, yet the CCC is devoid of sufficient individualized facts. *Griffin v. Dugger*, 823 F.2d 1476, 1482–83 (11th Cir. 1987) (“[A] plaintiff

must allege and show that he personally suffered injury.... [A] plaintiff cannot include class action allegations in a complaint and expect to be relieved of personally meeting the[se] requirements....”). For efficiency, in this Memorandum, Equifax has put Plaintiffs into categories corresponding to the basic types of harms they allege. See Ex. 1 (table summarizing which allegations of harm each Plaintiff has raised). And as shown below, Plaintiffs’ alleged harms largely do not amount to *legally cognizable* injuries.

a. *Compromise of PII.* All Plaintiffs allege that their PII was compromised in the data breach. See CCC ¶¶ 13–108; see also Table (Ex. 1). But in Georgia, the “compromise” of PII is not enough to support a claim. See, e.g., *Rite Aid of Ga., Inc. v. Peacock*, 726 S.E.2d 577, 580 (Ga. Ct. App. 2012) (plaintiff “suffered no injury” from allegedly illegal sale of PII); *Finnerty v. State Bank & Trust Co.*, 687 S.E.2d 842, 845 (Ga. Ct. App. 2009), *disapproved in part on other grounds by Cumberland Contractors, Inc. v. State Bank & Trust Co.*, 755 S.E.2d 511 (Ga. Ct. App. 2014); see also *Pisciotta v. Old Nat’l Bancorp.*, 499 F.3d 629, 634–35, 640 (7th Cir. 2007) (affirming dismissal of negligence claim in data-breach suit because “the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft” do not support a claim for negligence). In *Finnerty*, for example, the Georgia Court of Appeals held that the

release of a Social Security number was not a sufficient injury to state a claim for negligence—even though the plaintiff alleged “increased risk of identity theft” and that “non-authorized third parties [had] access to ... otherwise confidential personal information.” 687 S.E.2d at 845 (quotation marks omitted). Just so here: the alleged compromise of Plaintiffs’ PII is not a legally cognizable injury under Georgia law.

b. Unspecified Future Harms. All Plaintiffs further allege that they are at a “substantial and imminent risk” of unspecified “future harm.” See CCC ¶¶ 13–108; see also Table (Ex. 1). But Plaintiffs’ “fear of future damages [from identity theft] is too speculative to form the basis for recovery.” *Finnerty*, 687 S.E.2d at 845; *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708 n.9 (D.C. 2009) (collecting cases holding that the “absence of allegations of present injury” is fatal to plaintiffs’ tort claims). And Plaintiffs plead no facts demonstrating that any future harm is “substantial” or “imminent”—to the contrary, it is not likely that any Plaintiff will suffer future harm from the Equifax data breach. See *infra* Section I.B.2; *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (“data breaches are unlikely to result in account fraud”) (discussing GAO Report GAO-07-737).

c. Mitigation of Future Harms. Many Plaintiffs allege that they had to spend “time and effort” to mitigate future harm from the data breach. *E.g.*, CCC

¶¶ 17, 21, 57; *see also* Table (Ex. 1). Some Plaintiffs also allege that they spent money to mitigate the risk of future harm—*e.g.*, by buying credit monitoring or identity theft insurance (despite Equifax offering these services for free to all U.S. consumers). *E.g.*, CCC ¶¶ 22, 46, 54; *see also* Table (Ex. 1). But “[t]he majority of courts in data breach cases have held that the cost to mitigate the risk of future harm does not constitute an injury ... unless the future harm being mitigated against is itself imminent.” *Torres v. Wendy’s Co.*, 195 F. Supp. 3d 1278, 1284 (M.D. Fla. 2016) (quotation marks omitted); *see also SuperValu*, 870 F.3d at 771; *Randolph*, 973 A.2d at 708 n.9. Here, since the CCC is devoid of facts suggesting that any harm is imminent or even likely—*e.g.*, facts showing that the criminal hackers intend to use Plaintiffs’ PII to commit more crimes—Plaintiffs cannot rely on time and money spent mitigating those theoretical future harms as an injury.

d. Payment-Card Fraud. Plaintiffs Kleveno, Martucci, and Etten allege that their payment-card numbers were compromised and that they later suffered fraudulent charges.⁵ CCC ¶¶ 26, 33, 60. None of those Plaintiffs, however, allege the date on which any fraudulent charges were made or that he has not been reimbursed for those charges. *See id.* As a result, these Plaintiffs have failed to

⁵ Plaintiff Crowell also alleges that his payment card was compromised but does not allege fraudulent charges. ¶ 80. Instead, he alleges only time and effort—not money—spent in hope of mitigating future harms. *Id.*

plead a cognizable injury at all—much less one resulting from the Equifax data breach. *See, e.g., Provost v. Aptos, Inc.*, No. 1:17-cv-02120-ELR, 2018 WL 1465766, at *3 (N.D. Ga. Mar. 12, 2018) (plaintiff who failed to allege that “she requested reimbursement from her bank or that she was denied such reimbursement” suffered no injury); *Torres*, 195 F. Supp. 3d at 1282–83 (plaintiff who did not allege “charges went unreimbursed by his credit union” had “not alleged any monetary harm” from fraudulent charges); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1283, 1285 (N.D. Ala. 2014) (when fraudulent charges were reimbursed, plaintiff suffered no actual injury).

This theory of injury, moreover, does not apply to the overwhelming majority of Plaintiffs or putative class members. As Plaintiffs concede, just a fraction (less than one fifth of one percent) of affected consumers’ stolen records included payment-card information. CCC ¶ 212.

2. Independently, Plaintiffs Have Failed To Allege That Equifax Proximately Caused Their Alleged Injuries.

Under Georgia law, “[i]f the damage incurred by the plaintiff is only the ... possible result of a tortious act or if other and contingent circumstances preponderate in causing the injury, such damage is too remote to be the basis of recovery against the wrongdoer.” O.C.G.A. § 51-12-8. Thus, a “wrongdoer is not responsible for a consequence which is merely possible, according to occasional

experience, but only for a consequence which is probable, according to ordinary and usual experience.” *Morris v. Baxter*, 483 S.E.2d 650, 651 (Ga. Ct. App. 1997).

Plaintiffs fail to allege that any damages from identity theft, payment-card fraud, or similar theories resulted from the Equifax data breach and not some other data breach or fraudulent activity. Plaintiffs highlight “dozens” of other data breaches dating back to 2013 in which the PII of billions of individuals was stolen. CCC ¶¶ 160–65. Indeed, 2017 alone saw 1,579 data breaches across the United States. *See* Fin. Inst. Pls.’ Consol. Am. Compl. ¶ 139 (May 30, 2018), ECF No. 390 (citing Identity Theft Resource Ctr., 2017 End of Year Report, at 6 (2018), <https://bit.ly/2sCibRG>). Importantly, *no* Plaintiff alleges that her PII was *not* stolen in other data breaches. *See generally* CCC. Given how often data breaches occur, Plaintiffs’ attempt to blame Equifax is guesswork at best. *Morris*, 483 S.E.2d at 651. Certainly, no individual Plaintiff has alleged (or could allege) *facts* tying any actual harm to the Equifax breach.

In any event, Plaintiffs have not alleged that *Equifax* is itself directly responsible for any injury. Instead, each of the injuries Plaintiffs allege was proximately caused by an unidentified third party’s criminal acts—breaking into Equifax’s servers and stealing information stored on them. *See* 18 U.S.C. § 1030(a)(5)(C) (making it a federal crime to “intentionally access[] a protected

computer without authorization”). Unforeseeable criminal acts of third parties “insulat[e] and exclud[e] the negligence of the defendant” from liability. *Goldstein, Garber & Salama, LLC v. J.B.*, 797 S.E.2d 87, 89 (Ga. 2017) (quotation marks omitted). And criminal acts are foreseeable only if they are the “probable or natural consequences” of “the original wrongful act.” *Id.* at 89–90; *see also id.* at 90–91 (mere “aware[ness]” that an event “can occur” does not create liability).

In *Andrews v. Kinsel*, 40 S.E. 300 (Ga. 1901), a store lessee sued its landlord after the store was burglarized. The landlord had left windows in an adjoining store open and had also taken down a partition between the two stores. *Id.* at 300. The lessee alleged that leaving open the partition and windows, and that failing to notify the lessee that the store was open, constituted negligence that proximately caused the lessee’s injuries. *Id.* The Georgia Supreme Court disagreed, holding that “there intervened as a direct cause between the negligence of the defendant and the damage sustained by [plaintiffs] the independent criminal act of a responsible human agency,” and so the trial court should have dismissed the case. *Id.* at 301. Under *Andrews*, Plaintiffs’ strained theory of proximate causation fails.

Nor has any Plaintiff pleaded that any *future* identity theft or fraud is a probable consequence of the data breach. Plaintiffs have failed to plead facts that show that identity fraud is *likely* to result when a consumer’s PII is compromised,

see SuperValu, 870 F.3d at 771, and any such harm would necessarily involve a *second* intervening criminal act in any case, *see* 18 U.S.C. § 1028, further attenuating any causal connection to the breach. *See Andrews*, 40 S.E. at 301.

3. Economic Loss Doctrine.

Even if Plaintiffs’ allegations of injury and causation were otherwise sufficient, the economic loss doctrine bars their tort claims. In *General Electric Co. v. Lowe’s Home Centers, Inc.*, 608 S.E.2d 636, 637 (Ga. 2005), the Georgia Supreme Court held that “[u]nder the economic loss rule, a [contracting party] can recover in tort *only* those economic losses resulting from injury to his person or damage to his property.” (Emphasis added.) And in *Remax Mountain Co. v. Tabsum, Inc.*, 634 S.E.2d 77, 79 & n.6 (Ga. Ct. App. 2006), *cert. denied* Nov. 6, 2006, the Court of Appeals held that the economic loss rule bars tort claims for economic damages even where no contract exists. No Plaintiff has alleged any personal injury or property damage (nor could they). *See* CCC ¶¶ 13–108 & 294(a)–(k). All Plaintiffs’ tort claims should therefore be dismissed. *See, e.g., Willingham v. Global Payments, Inc.*, No. 1:12-cv-01157-RWS, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013) (King, Mag. J. R. & R.). At a minimum, because they had a contract with Equifax, *see infra* Section II.A, the Contract Plaintiffs’ tort claims must be dismissed. *See Lowe’s*, 608 S.E.2d at 637.

C. Plaintiffs’ Negligence And Declaratory Judgment Claims Must Be Dismissed.

To succeed on a negligence claim, a plaintiff must prove “the existence of a duty on the part of the defendant, a breach of such duty, causation of the injury alleged, and damages as a result of the alleged breach of duty.” *Wells Fargo Bank, N.A. v. Jenkins*, 744 S.E.2d 686, 687 (Ga. 2013). Because Georgia law imposes no legally applicable duty to safeguard PII, Plaintiffs cannot maintain their negligence claims. The absence of a duty also defeats their claim for a declaratory judgment.

1. Georgia Law Does Not Impose Any Applicable Duty Of Care, So Plaintiffs’ Negligence And Declaratory Judgment Claims Must Be Dismissed.

a. Georgia Law Imposes No Relevant Duty Of Care. “The threshold issue in any cause of action for negligence is whether, and to what extent, the defendant owes the plaintiff a duty of care.” *Access Mgmt. Grp., L.P. v. Hanham*, 812 S.E.2d 509, 512 (Ga. Ct. App. 2018) (quotation marks omitted). Whether a duty exists is a question of law. *Id.*

The Georgia Court of Appeals recently decided the legal question central to Plaintiffs’ negligence claim, holding that “a duty of care to safeguard personal information ... has *no source* in Georgia statutory law or caselaw.” *See McConnell v. Ga. Dep’t of Labor*, — S.E.2d —, No. A16A0655, 2018 WL 2173252, at *6 (Ga. Ct. App. May 11, 2018), *cert. pending* (“*McConnell III*”)

(emphasis added). Plaintiffs’ negligence claim accordingly fails at the threshold. And Plaintiffs’ claim for declaratory judgment, which seeks a declaration that Equifax owed a “dut[y] to reasonably safeguard its customers’ Personal Information,” fails for the same reason. *See* CCC ¶¶ 392–99 (Count 6).

In *McConnell*, an employee of the Georgia Department of Labor sent an email to over 1,000 recipients containing the PII of over 4,000 individuals, including their names, Social Security numbers, ages, phone numbers, and email addresses. *McConnell III*, 2018 WL 2173252, at *1. One of the individuals whose information was exposed brought a putative class action against the Department alleging, among other things, that the Department was negligent in disclosing the PII. *Id.* at *1, *5. The trial court dismissed the action on multiple grounds, including that the Department had sovereign immunity and that the plaintiff failed to state a claim under Georgia law. *Id.* at *1. In a June 2016 opinion, the Court of Appeals affirmed the dismissal for failure to state a claim—holding that no common-law or statutory duty exists under Georgia law to safeguard another’s personal information. *McConnell v. Dep’t of Labor*, 787 S.E.2d 794, 799 (Ga. Ct. App. 2016) (“*McConnell I*”). The Georgia Supreme Court later vacated *McConnell I* solely on the ground that the court should have considered the trial court’s sovereign-immunity ruling, a question of subject-matter jurisdiction, before

addressing the duty question. *McConnell v. Dep’t of Labor*, 805 S.E.2d 79, 79–80 (Ga. 2017) (“*McConnell II*”).

On remand, in an opinion issued May 11, 2018, the Court of Appeals first addressed subject-matter jurisdiction as instructed and held that sovereign immunity did not bar the plaintiff’s claims. *McConnell III*, 2018 WL 2173252, at *4.⁶ The court thus again addressed the merits and, with respect to the negligence claim, reaffirmed its holding that Georgia law does not permit a negligence claim to proceed on the theory that the defendant failed to safeguard plaintiff’s PII. *Id.* at *6. To succeed on a negligence claim, the court explained, a plaintiff must prove “the existence of a duty on the part of the defendant, a breach of that duty, causation of the alleged injury, and damages resulting from the alleged breach of the duty.” *Id.* at *5 (quotation marks omitted). The duty must arise “either from a valid legislative enactment, that is, by statute, or be imposed by a common law principle recognized in the caselaw.” *Id.* (quotation marks omitted). Because a duty to safeguard PII “has no source in Georgia statutory law or caselaw,” the court held, the plaintiff had failed to state a claim. *Id.* at *6.

⁶ One judge specially concurred in the panel’s sovereign immunity holding, rendering that portion of case “physical precedent only.” Ga. Ct. App. R. 33.2(a)(1); *McConnell III*, 2018 WL 2173252, at *10. All judges concurred fully in the remainder of the opinion, making those portions—including the negligence holding—“binding precedent” in Georgia. *See* Ga. Ct. App. R. 33.2(a)(1).

b. *McConnell III Is Binding.* A federal Court sitting in diversity must “decide the case the way it appears the [Georgia] Supreme Court would decide it.” *KMS Rest. Corp. v. Wendy’s Int’l, Inc.*, 361 F.3d 1321, 1325 (11th Cir. 2004). And “[i]n the absence of any [Georgia] Supreme Court decisions close enough on point,” the Court must “look to decisions of the [Georgia] intermediate appellate courts and follow them unless there is some *really persuasive* indication that the [Georgia] Supreme Court would go the other way.” *Id.* (emphasis added). Absent “persuasive evidence that the [Georgia Supreme Court] would rule otherwise,” this Court is “bound” to follow the Georgia Court of Appeals’ decision. *Bravo v. United States*, 577 F.3d 1324, 1326 (11th Cir. 2009) (quotation marks omitted).

Here, there is no “really persuasive indication” that *McConnell III*’s duty analysis is wrong. *See KMS Rest. Corp.*, 361 F.3d at 1325. To the contrary, *McConnell III* is fully in line with the Georgia Supreme Court’s decisions on the question of duty. In *Jenkins*, 744 S.E.2d at 687–88, the Georgia Supreme Court rejected the plaintiff’s argument that Georgia law imposes a duty to protect another’s PII. *Id.* at 688. The court concluded that the federal Gramm-Leach-Bliley Act’s “aspirational statement of Congressional policy” was not sufficient to impose a duty, “the alleged breach of which would give rise ... to a cause of action for negligence,” to guard against unauthorized access to confidential information.

Id. The *Jenkins* court further concluded that it would not craft this new duty itself—indicating that none exists at Georgia common law—and cautioned against “usurp[ing] legislative authority by inferring or supplying” a duty not found in statutory or existing case law. *Id.*

In line with that caution, the Georgia Supreme Court has explicitly rejected lower courts’ fashioning of new common-law duties. *See, e.g., Albany Urology Clinic, P.C. v. Cleveland*, 528 S.E.2d 777, 780 (Ga. 2000). In *Cleveland*, the Supreme Court reversed the Georgia Court of Appeals’ “impos[ition] upon healthcare providers [of] a new, judicially-created[] duty” because creating such a duty was “beyond the scope of the appellate court’s authority.” *Id.* at 780. The Supreme Court reversed the lower court “notwithstanding the repugnance” of the defendant doctor’s conduct—the abuse of cocaine while treating the plaintiff patient, who suffered “acutely painful” injuries from the doctor’s botched surgery. *Id.* at 778–80. That the Georgia Supreme Court rejected the imposition of a new duty on those facts demonstrates that the court would be unlikely to recognize any new duty here, where Plaintiffs lacking any relationship with Equifax allege nothing more than economic harms—most of them speculative.

The Georgia Supreme Court has also recognized that a court “fixing the bounds of duty” must limit a tortfeasor’s responsibility for “wrongs ... to a

controllable degree.” *CSX Transp., Inc. v. Williams*, 608 S.E.2d 208, 209 (Ga. 2005) (quotation marks omitted). A court should not “expand traditional tort concepts beyond manageable bounds” when that would “create an almost infinite universe of potential plaintiffs.” *Id.* (quotation marks omitted). The expansive new duty urged by Plaintiffs would yield an “almost infinite universe of potential plaintiffs” in this case alone—not to mention when similarly broad classes of plaintiffs sue other defendants when other data-security breaches inevitably occur.

c. McConnell III Clarified The Law On Which This Court’s Earlier Rulings Relied. *McConnell III* provides reason to revisit this Court’s decisions in *In re Home Depot Customer Data Sec. Breach Litig.*, No. 1:14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016), and *In re Arby’s Rest. Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018).

In *Home Depot*, this Court ruled that Home Depot owed to “a putative class of financial institutions that issued and owned payment cards compromised by [Home Depot’s] data breach” a duty to safeguard payment-card data. 2016 WL 2897520, at *2. But *Home Depot* does not control here, for several reasons. First, *Home Depot* is distinguishable on its facts because the plaintiffs there were financial institutions whose payment-card information was breached. Financial institutions’ relationships with retailers like Home Depot are governed by contracts

with card brands. *See Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 808 (7th Cir. 2018). But here, the vast majority of Plaintiffs—and “nearly all” members of the putative nationwide class—have no direct relationship, contractual or otherwise, with Equifax.⁷ *See* CCC ¶ 4.

Second, *McConnell III* clarified the law on which *Home Depot*’s duty ruling was based. In *Home Depot*, this Court reasoned that a duty to safeguard PII arose from broad language in *Bradley Center, Inc. v. Wessner*, 296 S.E.2d 693, 695 (Ga. 1982), to the effect that defendants owe a “general duty to all the world not to subject them to an unreasonable risk of harm.” *Home Depot*, 2016 WL 2897520, at *3 (quotation marks omitted). Georgia courts, however, have repeatedly limited *Wessner* to its facts.⁸ At least one federal Court of Appeals concluded even before

⁷ And as discussed above, *see* Section I.B.3, *supra*, Contract Plaintiffs cannot maintain a tort action against Equifax under the economic loss rule.

⁸ *See Miranda v. Fulton DeKalb Hosp. Auth.*, 644 S.E.2d 164, 168–69 (Ga. Ct. App. 2007), *cert. denied* June 25, 2007 (rejecting negligence claim citing *Wessner* because there was “no long-standing relation between” plaintiff and defendant); *Walton v. UCC X, Inc.*, 640 S.E.2d 325, 329 (Ga. Ct. App. 2006), *cert. denied* Mar. 26, 2007 (rejecting negligence claim because “[t]he control that the defendant exercised over the mental patient in *Wessner* is lacking here”); *Houston v. Bedgood*, 588 S.E.2d 437, 440 (Ga. Ct. App. 2003), *cert. denied* Feb. 2, 2004 (negligence claim lacking element of control “reflects a fundamental misunderstanding of *Wessner*”); *Purcell v. Breese*, 552 S.E.2d 865, 868 (Ga. Ct. App. 2001), *cert. denied* Jan. 10, 2002 (rejecting *Wessner* theory of liability because “privity” existed between plaintiff and defendant); *Ermutlu v. McCorkle*, 416 S.E.2d 792, 794–95 (Ga. Ct. App. 1992), *cert. denied* Apr. 24, 1992

McConnell III that the vacated *McConnell I* decision indicated that *Home Depot's* “prediction of Georgia law ... seems to have been incorrect.” *Schnuck Mkts.*, 887 F.3d at 819 & n.8. *McConnell III* erases any lingering doubt: *Wessner* simply does not impose the duty Plaintiffs allege Equifax owed.

In *Arby's*, this Court expanded on *Home Depot*, concluding that defendant *Arby's* owed a duty to safeguard its customers' personal data. *See* 2018 WL 2128441, at *3–7. The *Arby's* Court considered and rejected the reasoning of *McConnell I*. First, *Arby's* noted that *McConnell I* had been vacated. 2018 WL 2128441, at *6. After *McConnell III*, that justification is no longer valid.

Second, the *Arby's* Court attempted to distinguish *McConnell* from *Home Depot* on its facts. *Id.* It reasoned that, unlike the *Home Depot* plaintiffs, Mr. McConnell had not pleaded facts demonstrating that the disclosure of his PII was foreseeable (*e.g.*, facts that the Department of Labor was on notice that it needed to implement better security measures). *See* 2018 WL 2128441, at *6. But under Georgia's notice-pleading standard, McConnell would not have been required to plead detailed allegations of foreseeability; instead, he would have been entitled to

(describing *Wessner* test as “determining under what circumstances a physician may be liable to a third party”); *Driebe v. Cox*, 416 S.E.2d 314, 316 (Ga. Ct. App. 1992), *cert. denied* Apr. 6, 1992 (rejecting *Wessner* argument due to lack of “foreseeability”); *Baldwin v. Hosp. Auth. of Fulton Cty.*, 383 S.E.2d 154, 156–57 (Ga. Ct. App. 1989) (rejecting *Wessner* argument because “none of the defendants ... ever had ‘control’” of third party patient and harm was unforeseeable).

develop those facts during discovery. *See id.* at *5. The holding of *McConnell III*, in short, does not stand only for the narrow rule that there is no duty in the context of an *unforeseeable* data breach. Rather, its holding is broad and fatal to Plaintiffs’ claim: Georgia law does not impose “a standard of conduct intended to protect the security of personal information.” *Id.* at *7.

d. Plaintiffs Fail to Allege any Other Cognizable Common Law Duty. To support their negligence claim, Plaintiffs also appear to suggest that Equifax voluntarily undertook a duty. *See, e.g.,* CCC ¶ 338–39. But while Equifax recognizes the importance of safeguarding consumers’ data, this claim fails as a matter of law. Georgia has adopted Section 324A of the Restatement (Second) of Torts governing an undertaking to protect another’s property. *See Pate v. Oakwood Mobile Homes, Inc.*, 374 F.3d 1081, 1086 (11th Cir. 2004). Under that “good Samaritan” provision, an undertaken duty extends only to preventing “*physical harm*” to another’s person or property. Restatement (Second) of Torts §§ 323, 324A (emphasis added); *see also Huggins v. Aetna Cas. & Sur. Co.*, 264 S.E.2d 191, 192 (Ga. 1980) (adopting “majority rule” of Restatement § 324A); *Willingham*, 2013 WL 440702 at *18. Plaintiffs allege no physical injury to themselves or their property. *See* CCC ¶¶ 13–108 (individual plaintiffs’ allegations of harm) & 294(a)–(k) (generalized allegations of harm). Nor does

Plaintiffs’ allegation that Equifax contractually requires *its business partners* to safeguard information, *see* CCC ¶¶ 341–42, show that Equifax undertook a legal duty owed *to Plaintiffs*.

Because Georgia law does not impose the duty Plaintiffs allege, their negligence and declaratory judgment claims (Counts 2 and 6) fail.

2. The FCRA Imposes No Relevant Duty Of Care.

Plaintiffs allege a duty “based on the FCRA” to “maintain reasonable procedures designed to avoid unauthorized release of information contained in consumer reports.” This allegation of duty is merely Plaintiffs’ defective FCRA claims—suggesting that Equifax furnished consumer reports to the attackers—recast as a tort. But as explained above, Equifax did not “furnish” any information, nor did the stolen information constitute “consumer reports.” This Court should accordingly reject this theory for the same reasons it should reject Plaintiffs’ FCRA claims. *See supra* Section I.A.

3. No Equifax Act Or Omission Proximately Caused Any Cognizable Injury To Plaintiffs.

As discussed above, Plaintiffs have failed to sufficiently allege any legally cognizable harm that was proximately caused by Equifax. *See supra* Sections I.B.1 & I.B.2. The failure to sufficiently allege causation or injury is fatal to a negligence claim. *See Jenkins*, 744 S.E.2d at 687.

D. Plaintiffs’ Negligence *Per Se* Claim Must Be Dismissed.

Plaintiffs allege that “Equifax violated Section 5 of the FTC Act (and [unspecified] similar state statutes),” and that this violation “constitutes negligence *per se*.”⁹ CCC ¶ 350. Because Plaintiffs do not identify any statute imposing a specific duty of care to safeguard personal information, and because in any event, they have failed to allege injury or causation, this Court should dismiss Count 3.

1. Plaintiffs Cannot Maintain A Negligence *Per Se* Action Under The Statutes They Cite.

Georgia law limits negligence *per se* to statutes that “provide for *certain* duties” or that call for “the performance of ... *specific* acts.” *Jenkins*, 744 S.E.2d at 688 (emphasis added). A claim that a defendant violated a statute whose duty is “too indefinite” cannot “constitute negligence *per se*.” *Brock v. Avery Co.*, 110 S.E.2d 122, 126 (Ga. Ct. App. 1959) (quotation marks omitted). Instead, any duty must be “imposed *expressly* by the statute at issue with specificity.” *Bellsouth Telecommc’ns LLC v. Cobb Cty.*, 802 S.E.2d 686, 698 (Ga. Ct. App. 2017) (Dillard, P.J., concurring), *cert. granted* Apr. 16, 2018. Further, the duty must be

⁹ Plaintiffs press substantially the same claim as part of their negligence count. CCC ¶ 337. But a claim that a statute supplies a duty of care for negligence purposes is in fact a claim for negligence *per se*. *See, e.g., Norman v. Jones Lang Lasalle Ams., Inc.*, 627 S.E.2d 382, 388 (Ga. Ct. App. 2006) (“negligence *per se* arises when a statute or ordinance is violated.”). The negligence claim thus fails for the same reasons discussed here.

based on violation of a rule that has “the force of law.” *Norman v. Jones Lang Lasalle Ams., Inc.*, 627 S.E.2d 382, 388 (Ga. Ct. App. 2006) (quotation marks omitted).

Here, Plaintiffs identify no statutory text imposing with specificity any duty they allege. Instead, they point broadly to Section 5 of the FTC Act “and similar state statutes” to contend that those statutes impose a legal duty to safeguard PII. But the FTC Act does not impose any such duty. *See generally* 15 U.S.C. § 45. It only proscribes “unfair or deceptive acts or practices in or affecting commerce.” *Id.* That prohibition is not specific enough to recover for negligence *per se*. *See Jenkins*, 744 S.E.2d at 688; *Brock*, 110 S.E.2d at 126.

Moreover, Section 5 does not impose substantive requirements unless they are established elsewhere in the law. *LabMD v. Fed. Trade Comm’n*, — F.3d —, No. 16-16270, — F.3d —, 2018 WL 3056794, at *7 (11th Cir. June 6, 2018). To be “unfair” under Section 5, an act must violate “clear and well-established policies that are expressed in the Constitution, statutes, or the common law.” *Id.* (quotation marks omitted). And, as the Eleventh Circuit held, the only possible “source of [a] standard of unfairness ... holding that ... [a] failure to ... maintain a reasonably designed data-security program constitute[s] an unfair act or practice.... is the common law.” *Id.* The common law, however, imposes no such duty.

McConnell III, 2018 WL 2173252, at *6. This Court therefore should not read such a duty into Section 5 of the FTC Act.¹⁰ *See LabMD*, 2018 WL 3056794, at *7.

And, for that matter, no private cause of action exists for violation of the FTC Act. *Fulton v. Hecht*, 580 F.2d 1243, 1248 n.2 (5th Cir. 1978). Instead, only the FTC may pursue an action under Section 5. “The express provision of one method of enforcing a substantive rule suggests that Congress intended to preclude others.” *Alexander v. Sandoval*, 532 U.S. 275, 290 (2001). Permitting a private plaintiff to sue for negligence *per se* under the FTC Act would undermine Congress’s express intent that private plaintiffs not be allowed to sue to enforce it.

The sole Georgia case permitting a negligence *per se* claim to go forward based in part on the FTC Act is not to the contrary. *See Legacy Acad., Inc. v. Mamilove, LLC*, 761 S.E.2d 880, 891 (Ga. Ct. App. 2014), *vacated in part on other grounds*, 771 S.E.2d 868 (Ga. 2015) & *reversed in part on other grounds on remand*, 777 S.E.2d 731 (Ga. Ct. App. 2015). There, the court permitted the claim only because the defendant did not dispute that it owed a duty, and Plaintiff alleged

¹⁰ Equifax is aware that this Court has ruled that a negligence *per se* claim relying on Section 5 of the FTC Act can proceed. *Arby’s*, 2018 WL 2128441, at *7–8; *Home Depot*, 2016 WL 2897520, at *4. Equifax respectfully suggests that both this case’s distinct factual circumstances and the Eleventh Circuit’s intervening *LabMD* case provide reason not to follow those rulings here.

the defendant violated a specific FTC regulation—one that explicitly made a franchisor’s failure to make certain disclosures to a franchisee “an unfair or deceptive trade practice in violation of” the FTC Act. *Id.* at 891 (citing 16 C.F.R. § 436.2) & 892 n.25. Because that regulation independently has “the force and effect of law,” *see Perez v. Mortg. Bankers Ass’n*, 135 S. Ct. 1199, 1203 (2015), and imposes a *specific* conduct requirement, it renders a negligence *per se* claim permissible under Georgia law. *Jenkins*, 744 S.E.2d at 688; *Norman*, 627 S.E.2d at 388; *Brock*, 110 S.E.2d at 126.

Here, by contrast, Plaintiffs point to no similar FTC regulation that requires safeguarding PII. Instead, they merely claim that the FTC has “pursued” numerous “enforcement actions” for “failure to employ reasonable data security measures.” CCC ¶ 353. Plaintiffs also point to unidentified “FTC publications and data security breach orders.” *Id.* ¶ 337. None of these various unidentified orders and publications can support a negligence *per se* claim because Plaintiffs have identified none that “ha[s] the force of law.” *Norman*, 627 S.E.2d at 388.

Similarly, although Plaintiffs allege negligence *per se* under “state statutes,” they do not identify them. *See* CCC ¶¶ 348–54. Accordingly, that claim too is insufficiently specific to state a negligence *per se* claim under Georgia law. *See Jenkins*, 744 S.E.2d at 688; *Brock*, 110 S.E.2d at 126.

2. Plaintiffs Have Not Sufficiently Alleged Injury Or Proximate Causation.

Under Georgia law, negligence *per se* “is not liability *per se*”—a “plaintiff must still prove proximate cause and actual damage in order to recover.” *Hite v. Anderson*, 643 S.E.2d 550, 552 (Ga. Ct. App. 2007) (quotation marks omitted). Here, Plaintiffs allege that Equifax’s purported negligence *per se* caused the same injuries as its alleged negligence. CCC ¶ 354 (cross-referencing to harm alleged under negligence claim in ¶ 347). But as discussed above, Plaintiffs have failed to allege sufficient facts demonstrating that they have suffered any cognizable injury proximately caused by Equifax. *See supra* Sections I.B.1 & I.B.2. As a result, their negligence *per se* claim must also be dismissed.

E. Plaintiffs’ Georgia Fair Business Practices Act Claim Must Be Dismissed.

1. *McConnell III* Confirms That The Georgia Fair Business Practices Act Does Not Require Safeguarding PII.

If the Georgia Fair Business Practices Act (“GFBPA”) required a company to safeguard PII, *McConnell III* would have been decided differently. The plaintiff in *McConnell* argued that the GFBPA imposed a duty to safeguard PII. *See McConnell III*, 2018 WL 2173252, at *6. And although the GFBPA was before the court, *McConnell III* held that the plaintiff’s complaint was “premised on a duty of care to safeguard personal information that has *no source in Georgia*

statutory law.” 2018 WL 2173252 at *6 (emphasis added). According to *McConnell III*, “[Georgia’s] legislature has so far not acted to establish a standard of conduct intended to protect the security of personal information.” *Id.* at *7. If the general unfair-practices provision of the GFBPA could be read to require safeguarding PII, the *McConnell III* court would have said as much—and would have reached a different result. This alone requires that Count 4 be dismissed.

2. Plaintiffs Have Not Pleaded Reliance.

Stating a claim under the GFBPA requires that the plaintiff “demonstrate that he was injured as the result of ... reliance upon the alleged misrepresentation.” *Tüsmann v. Linda Martin Homes Corp.*, 637 S.E.2d 14, 16–17 (Ga. 2006). Plaintiffs here have failed to—and cannot—allege facts sufficient to show reliance.

Most Plaintiffs—and “[n]early all” putative Nationwide Class members—allege that they did *not* provide their PII to Equifax.¹¹ For example, Plaintiffs allege that their “Personal Information was conferred on Equifax in most cases by third[] parties,” CCC ¶ 383, that they “had no prior relationship with Equifax,” and that they could not “opt[] out of Equifax’s collection ... of ... data,” CCC ¶ 4.

¹¹ Only Contract Plaintiffs allege that they provided any PII directly to Equifax, but those Plaintiffs have not sufficiently alleged that the PII they sent to Equifax was compromised in the breach. *See* CCC ¶¶ 400–01; *see also id.* ¶ 298 (defining putative “Contract Subclass” as “natural persons ... who ... transmitted directly to Equifax any of their Personal Information.”).

Under these facts, Plaintiffs cannot establish that they gave Equifax their PII in reliance on any representations Equifax allegedly made. This failure to plead reliance is fatal to the GFBPA claim.¹²

3. No Plaintiff Has Alleged Injuries Caused By Any Misrepresentation.

Plaintiffs have failed to allege cognizable injuries. *See supra* Section I.B.1. Those Plaintiffs who arguably have alleged injuries have failed to allege that Equifax proximately caused those harms. *See supra* Section I.B.2. To fall within the ambit of the GFBPA, a plaintiff must be a “person who suffers injury or damages as a result of a violation” of the act. O.C.G.A. § 10-1-399(a). Accordingly, because no Plaintiff has alleged “injury or damages as a result” of any violation by Equifax, Count 4 must be dismissed.

4. The GFBPA Forbids Class Actions.

The GFBPA forbids class actions. It provides that a “person who suffers injury or damages ... may bring an action individually, but not in a representative capacity.” O.C.G.A. § 10-1-399(a); *see also In re New Motor Vehicles Canadian*

¹² Even if Plaintiffs had given their PII to Equifax, they could not establish reliance because they have not pleaded that they read and relied on any representation made by Equifax. *See, e.g., Willingham*, 2013 WL 440702, at *20 (“[B]road statements of reliance on defendant’s website and privacy statement do not give rise to contract claims where, as here, Plaintiffs do not allege that they read and relied upon those statements.”).

Exp. Antitrust Litig., 241 F.R.D. 77, 84 (D. Me. 2007) (finding the GFBPA class action restriction substantive, not procedural, and rejecting class certification), *vacated on other grounds*, 522 F.3d 6 (1st Cir. 2008). Equifax therefore contends that this Court should dismiss Plaintiffs’ GFBPA claim as to any putative class.¹³ Equifax further notes that fifteen other state statutes under which Plaintiffs have asserted claims prohibit or restrict class actions, and those claims should also be dismissed as to any putative classes.¹⁴

F. Plaintiffs’ Unjust Enrichment Claim Must Be Dismissed.

To state a claim for unjust enrichment—an equitable doctrine of recovery under Georgia law—a plaintiff must allege that “the plaintiff provide[d] something of value to the defendant” and did so “*with the expectation that the defendant would be responsible for the cost thereof.*” *Sitterli v. Csachi*, 811 S.E.2d 454, 457 (Ga. Ct. App. 2018) (quotation marks omitted). Put another way, “when one

¹³ Equifax acknowledges that this Court is bound by Eleventh Circuit precedent holding that a similar provision in Alabama’s deceptive trade practices law is procedural, not substantive, and thus that Rule 23 governs. *See Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331, 1335 (11th Cir. 2015). At a minimum, however, *Lisk* presents a conflict in authority that either the *en banc* Eleventh Circuit or the Supreme Court could resolve in Equifax’s favor. *Compare id. with Fejzulai v. Sam’s West, Inc.*, 205 F. Supp. 3d 723, 726–29 (D.S.C. 2016) (disagreeing with *Lisk*); *In re New Motor Vehicles*, 241 F.R.D. at 84.

¹⁴ Each of Counts 10, 14, 31, 37, 41, 43, 51, 54, 57, 72, 76, 81, 86, 89, and 92 is premised on a state statute that forbids or otherwise limits class actions.

renders service or transfers property which is valuable to another ... a promise is implied to pay the reasonable value thereof.” O.C.G.A. § 9-2-7.

Here, Plaintiffs allege that “Personal Information was conferred on Equifax in most cases by third[] parties.” CCC ¶ 383. Only the Contract Plaintiffs are alleged to have given any information to Equifax. *See id.* ¶ 298 (describing putative “Contract Subclass”).

Thus, all non-Contract Plaintiffs fail to allege that *they* conferred anything of value on Equifax. Because these Plaintiffs neither “render[ed] service” nor “transfer[red] property” to Equifax, O.C.G.A. § 9-2-7, they may not recover for unjust enrichment, *Sitterli*, 811 S.E.2d at 457. Likewise, the Contract Plaintiffs explicitly allege that a contract governed their transactions with Equifax. Contract Plaintiffs, therefore, cannot plead a claim for unjust enrichment. *See Clark v. Aaron’s, Inc.*, 914 F. Supp. 2d 1301, 1310 (N.D. Ga. 2012) (“a plaintiff may not plead an unjust enrichment claim in the alternative to a claim for breach of contract when it is undisputed (or when the court has found) that a valid contract exists”).

Regardless, *no* Plaintiffs—Contract Plaintiffs or otherwise—allege that they reasonably expected Equifax to “be responsible for the cost” of their PII. The closest Plaintiffs come is their allegation that “the benefit conferred upon ... Equifax was not conferred ... gratuitously.” CCC ¶ 390. But that conclusory

assertion does not allege that *Plaintiffs* reasonably expected reimbursement, that anyone expected reimbursement *from Equifax*, or that any expected reimbursement would be for *the cost* of the PII as opposed to some other measure of value. Accordingly, the Plaintiffs “ha[ve] no right to an equitable recovery” for unjust enrichment. *See Sitterli*, 811 S.E.2d at 457 (quotation marks omitted).

Finally, Plaintiffs seek, as damages, “the profits Equifax is receiving from the use and sale of” the PII. But the only damages available for unjust enrichment amount to the “reasonable value” of the “service” or “property” conferred. O.C.G.A. § 9-2-7. Plaintiffs cannot maintain an action for some other measure of damages. Plaintiffs’ unjust enrichment claim must be dismissed.

II. THE CONTRACT AND FCRA DISCLOSURE CLAIMS MUST BE DISMISSED.

A. Both Breach Of Contract Claims Must Be Dismissed.

Nineteen Plaintiffs¹⁵ allege that they had a contract with Equifax—either express or implied in fact—as a result of their purchase of Equifax credit monitoring or identity protection services, or other transactions with Equifax. CCC ¶¶ 405, 410. These Contract Plaintiffs allege that the purported contract

¹⁵ The Complaint alleges that “Thomas *Cromwell*” is a Contract Plaintiff for purposes of both Counts 7 and 8. CCC ¶¶ 400, 409. Equifax presumes for the purposes of this motion that the reference to Mr. Cromwell, who is not a named Plaintiff, is intended to refer to Plaintiff “Thomas Edward *Crowell*.” *Id.* ¶ 80.

consisted of or incorporated language from Equifax’s Privacy Policy, and that Equifax breached the contract by failing to protect Contract Plaintiff’s PII. *Id.* ¶¶ 401–04 & 410–15. Contract Plaintiffs’ allegations that the company’s Privacy Policy imposed contractual duties on Equifax are simply insufficient—indeed, these Plaintiffs’ transactions were governed by express contracts that do *not* incorporate the Privacy Policy and contain merger clauses.

1. The Privacy Policy Is Not A Contract, And Even If It Were It Does Not Impose The Duty Plaintiffs Assert.

The breach of contract claims fail for three reasons. *First*, Contract Plaintiffs’ purchases from Equifax were governed by an express contract that *does not* incorporate the Privacy Policy. *See generally* Equifax Terms of Service And Product Agreement, *available at* <https://bit.ly/2LVxNI0> (“Equifax Product Agreement”).¹⁶ The Equifax Product Agreement further provides that it “constitutes the entire agreement between You and” Equifax. Product Agreement ¶ 39. Because this “merger clause operates as a disclaimer of all representations not made on the face of the contract,” *Ekeledo v. Amporful*, 642 S.E.2d 20, 22 (Ga.

¹⁶ Plaintiffs rely on other terms of this agreement in the CCC. *E.g.*, CCC ¶¶ 233, 248. And because this agreement governs Contract Plaintiffs’ claims, the Court may consider it on a motion to dismiss. *See Bradford v. WR Starkey Mortg., LLP*, No. 2:06-CV-86-WCO, 2006 WL 8436036, at *4 (N.D. Ga. Nov. 17, 2006) (“incorporation by reference” is “properly used ... when the contents of a document are at issue in the case”).

2007), Plaintiffs’ allegation that Equifax’s Privacy Policy was incorporated into any contract they formed with Equifax fails.

Second, even if that express contract did not govern, Plaintiffs have not sufficiently alleged that the Privacy Policy is an enforceable contract between Plaintiffs and Equifax. Plaintiffs bear the burden of pleading all the elements of a contract. *Broughton v. Johnson*, 545 S.E.2d 370, 371 (Ga. Ct. App. 2001). To state a claim for breach of contract, a plaintiff must first “set forth a contract of such certainty and completeness that either party may have a right of action upon it.” *Weathers v. Dieniahmar Music, LLC*, 788 S.E.2d 852, 858 (Ga. Ct. App. 2016). Formation of a contract requires “mutual assent by all parties *to all contract terms*.” *Broughton*, 545 S.E.2d at 371 (emphasis added).

Contract Plaintiffs have not sufficiently pleaded that the Privacy Policy is part of any agreement they have with Equifax (or that it is itself an agreement). *See* ¶ 405. A plaintiff may not sue for “breach” of policies extrinsic to a contract unless the defendant assented to incorporating those policies into the contract. *E.g., Wilson v. Clark Atlanta Univ., Inc.*, 794 S.E.2d 422, 432 (Ga. Ct. App. 2016) (argument that handbook was incorporated into contract by reference failed because contract “does not make it reasonably clear that all provisions ... are incorporated ... thereby creating mutual obligations on” both parties).

Here, while Contract Plaintiffs allege that they “formed *a* contract” or “entered into *an* implied contract” with Equifax, CCC ¶¶ 405, 410, 412 (emphasis added), they nowhere explain whether or how the Privacy Policy provisions on which they rely became part of that contract. *Id.* Contract Plaintiffs certainly do not identify any specific contractual language—or append to their complaint any contract—making the Privacy Policy binding as between the parties. Plaintiffs have, therefore, failed to plead the existence of the contractual duty they rely on. *See Broughton*, 545 S.E.2d at 371; *see also In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 980–81 (N.D. Cal. 2016) (dismissing breach of contract claim where plaintiffs failed to allege that the privacy notices at issue had been incorporated into a valid contract); *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (“[B]road statements of company policy do not generally give rise to contract claims. As such, the alleged violation of the privacy policy at issue does not give rise to a contract claim.”); *In re Nw. Airlines Privacy Litig.*, No. Civ. 04-126(PAM/JSM), 2004 WL 1278459, at *5–6 (D. Minn. June 6, 2004) (finding no contract where plaintiffs alleged they relied on privacy policy on defendant’s website).

Third, even if Plaintiffs could show that the Privacy Policy governed, they cannot show that it imposed a contractual duty to safeguard information. All

versions of Equifax’s Privacy Policy provide that Equifax may, at any time, unilaterally alter the policy. For example, the version of the Privacy Policy quoted by Plaintiffs, effective as of 2006, provides that Equifax “may change [its] privacy policy in the future” and that it “may notify you of changes in [its] privacy policy through this web site.” See Privacy Policy, <https://bit.ly/2J5rXSg> (revised October 5, 2006). Equifax’s most recent Privacy Policy, therefore, applies. It became effective April 24, 2017, and thus was in effect during the entire period of the data breach. Privacy Policy—Equifax Personal Products, <https://bit.ly/2xvDU2o>.

That superseding Privacy Policy does not impose the contractual duty Plaintiffs allege. To the contrary, in a paragraph prominently and conspicuously titled “EFFORTS WE MAKE TO SAFEGUARD YOUR PERSONAL INFORMATION,” it provides:

We are committed to protecting the security of your personal information and use technical, administrative[,] and physical security measures that comply with applicable federal and state laws. However, no data transmission or storage can be guaranteed to be 100% secure. As a result, while we strive to protect the personal information we maintain, *we cannot ensure or warrant the security of any information you transmit to us.*

Privacy Policy—Equifax Personal Products (emphasis added). Thus, even if Plaintiffs had sufficiently alleged that the Privacy Policy imposed contractual obligations on Equifax (and they have not), at all times relevant to Contract

Plaintiffs' claims, the Privacy Policy expressly stated that Equifax could not "ensure or warrant the security of any information you transmit to us." *Id.* Because Equifax made clear that it was not taking on an enforceable duty to safeguard PII, Contract Plaintiffs' breach claim must be dismissed.

2. Plaintiffs Do Not Properly Allege Breach Of An Implied Contract.

Plaintiffs' alternative theory of breach of an *implied* contract is equally unavailing. The existence of an express contract with a merger clause governing Contract Plaintiffs' transactions with Equifax means that any "implied contract cannot exist." *In re VTech Data Breach Litig.*, No. 15-CV-10889, 2018 WL 1863953, at *3 (N.D. Ill. Apr. 18, 2018); *see also Ekeledo*, 642 S.E.2d at 22.

Nor would Plaintiffs' theory hold up even absent that express contract. Under a theory of "implied contract," Georgia courts require that that "the minds of the parties shall meet and accord at the same time, upon the same subject matter, and in the same sense." *Donaldson v. Olympic Health Spa, Inc.*, 333 S.E.2d 98, 100 (Ga. Ct. App. 1985); *see also Grange Mut. Cas. Co. v. Woodard*, 797 S.E.2d 814, 853 (Ga. 2017) ("[A]n implied contract only differs from an express contract in the mode of proof; both equally proceed upon the mutual agreement of the parties, and cannot exist without it.") (quotation marks omitted). That is particularly true in cases like this one, where Plaintiffs are alleging that Equifax

breached an implied duty to “safeguard” Plaintiffs’ PII from third-party criminals: “In the absence of a plain and explicit expression of willingness to protect another from the criminal acts of third parties, Georgia courts have refused to imply such a contractual obligation.” *Burnett v. Stagner Hotel Courts, Inc.*, 821 F. Supp. 678, 682 (N.D. Ga. 1993), *aff’d*, 42 F.3d 645 (11th Cir. 1994).

The Complaint describes only the following implied contract:

Plaintiffs and Class members entered into an implied contract with Equifax when they obtained credit monitoring or identity theft protection services from Equifax, or otherwise provided Personal Information to Equifax subject to its Privacy Policy (through obtaining disclosures of their credit files, disputing items in their credit files, or taking action associated with a fraud alert, active duty alert, or security freeze or lock on their credit files).

CCC ¶ 410. Plaintiffs then allege, in entirely conclusory fashion, that “Equifax agreed to safeguard and protect the Personal Information of Plaintiffs and Class Members and to timely and accurately notify them if their Personal Information was breached or compromised.” *Id.* ¶ 411. This is nothing more than a legal conclusion couched as fact. Absent from these allegations is any description of when these agreements were made, how Equifax manifested its assent to the terms, what individuals had a “meeting of the minds,” or any other allegations that would demonstrate the existence of an implied contract between Equifax and any of the Plaintiffs. Under these circumstances, Count 8 must be dismissed.

3. Plaintiffs Identify No Contractual Duty To “Promptly Alert Or Give Notice Of [A] Breach.”

Although the CCC alleges that Equifax “breached its agreement with [Contract] Plaintiffs” by “fail[ing] to promptly alert or give notice of the breach,” CCC ¶ 407, they have alleged no contract term that suggests Equifax made such a promise, *see id.* ¶¶ 402–04. Therefore, that claim must be dismissed.

B. The FCRA Disclosure Plaintiffs’ Claims Must Be Dismissed

Plaintiffs Cho and Lee assert, on behalf of a putative “FCRA Disclosure Subclass,” that Equifax violated 15 U.S.C. § 1681g(a) by failing to “clearly and accurately disclose” information about the data breach on consumer-credit-file disclosures issued since the breach. *See* CCC ¶ 419. Section 1681g(a) requires CRAs, upon request, to “clearly and accurately disclose to the consumer” “[a]ll information in the consumer’s file at the time of the request,” including the “[i]dentification of each person ... that procured a consumer report.” 15 U.S.C. § 1681g(a). An “identification of a person” who procures a consumer report must include “the name of the person ... ; and [] upon request of the consumer, the address and telephone number of the person.” *Id.* § 1681g(a)(3)(B).

As a threshold matter, Plaintiffs fail to plead facts showing that the *theft* of their PII was reflected in their “consumer[] file[s]” within the meaning of sections 1681a and 1681g. Thus, they cannot state a claim under § 1681g.

Independently, Plaintiffs' § 1681g claim fails because (1) the hackers did not "procure a consumer report," and thus did not trigger § 1681g's requirement that a consumer disclosure identify them; and (2) § 1681g cannot reasonably be read to apply in the context of a data breach.

First, for the same reasons discussed above, Plaintiffs' allegations show that the hackers did not access any "consumer report." That, alone, is fatal to the § 1681g claim—as it was fatal to Plaintiffs' claims under §§ 1681b and 1681e. *See supra* Section I.A; *Miller v. Experian Info. Sols. Inc.*, No. 3:13-cv-090, 2015 WL 728342, at *4–5, *8–9 (S.D. Ohio Feb. 19, 2015) (holding there is no violation of § 1681g unless a CRA issues a consumer report), *aff'd sub nom. Miller v. Trans Union, LLC*, 644 F. App'x 444 (6th Cir. 2016).

Second, a data breach does not trigger a CRA's § 1681g disclosure obligations. Section 1681g requires a CRA "upon request [to] ... clearly and adequately disclose to the consumer ... [i]dentification of each person ... that procured a consumer report ... for any [] purpose, during the one-year period preceding the date on which the request is made." 15 U.S.C. § 1681g(a)(3)(A). "[I]dentification of a person," in turn, requires disclosing the person's "name," "trade name," "address," and "telephone number." *Id.*; § 1681g(a)(3)(B).

Section 1681g(a)(3) clearly contemplates a third party—*e.g.*, a bank or

employer—obtaining a “consumer report” in the ordinary course of business. But it would be absurd to apply the provision where a CRA’s information systems were *hacked* in a data breach. If a data breach occurs, a CRA generally has no way of knowing—and thus cannot “clearly and accurately disclose”—the “name,” “trade name,” “address,” and “telephone number” of the criminal hackers who infiltrated its systems. *Id.* Congress could not have intended the statute to compel CRAs to disclose information they have no way of knowing.¹⁷ Because the FCRA Disclosure Plaintiffs’ claim rests on an unreasonable interpretation of the statute, Count 9 must be dismissed. *See, e.g., Clinton v. City of New York*, 524 U.S. 417, 429 (1998) (rejecting reading of a statute that ““would produce an absurd and unjust result which Congress could not have intended””); *Pub. Citizen v. U.S. Dep’t of Justice*, 491 U.S. 440, 454–55 (1989) (same).

III. EACH PLAINTIFF’S CLAIMS UNDER HIS OR HER LOCAL STATE STATUTES MUST BE DISMISSED.

Plaintiffs have raised a host of claims under state statutes, both individually

¹⁷ In their Complaint, Plaintiffs suggest that Equifax could “identify ... in general terms[] the person who procured” their PII. CCC ¶ 420. But § 1681g(a)(3)(A) requires CRAs to disclose details about anyone who accesses credit reports and does not contemplate that these details could ever be unknown. That Plaintiffs apparently concede that fully complying with § 1681g(a)(3)(A) is impossible in the context of a data breach is all the more reason to conclude that their reading of the statute is wrong.

and on behalf of putative Statewide Subclasses. These claims too must be dismissed. First, Plaintiffs seek to impermissibly apply foreign states' deceptive-trade-practices laws to conduct that undisputedly took place entirely in Georgia. Second, Plaintiffs fail to meet the requirements of those statutes—they have variously failed to sufficiently plead fraud, scienter, reliance, injury, or the existence of a requisite consumer transaction; or they seek money damages under statutes affording only nonmonetary relief. Third, Plaintiffs have brought several counts under data-breach-notification statutes that provide no private cause of action; have failed to (and cannot) sufficiently allege that Equifax violated any data-breach-notification statutes; and have failed to allege that any Plaintiff was injured by any delay in notification. And, fourth, Plaintiffs have asserted claims under certain statutes without alleging that any Plaintiff has any connection with the jurisdictions in question. Accordingly, all of Plaintiffs' state statutory claims must be dismissed.

A. Plaintiffs' Claims Under State Business Fraud And Consumer Protection Statutes Must Be Dismissed.

1. Foreign States' Deceptive-Trade-Practices Laws Cannot Govern Conduct That Took Place In Georgia.

By alleging claims under the deceptive-trade-practices laws of 49 other jurisdictions, Plaintiffs seek to impose foreign state statutes to govern conduct that

they allege occurred entirely in Georgia.¹⁸ See, e.g., CCC ¶ 311 (“Equifax’s breaches of duty ... emanated from Georgia.”). Those statutes, however, cannot be applied extraterritorially. As a matter of state law, state legislatures have no power to regulate conduct occurring in another state.¹⁹

Nor *could* states constitutionally reach out to govern conduct occurring elsewhere. See, e.g., *State Farm v. Campbell*, 538 U.S. 408, 421 (2003). Under

¹⁸ To the extent this Court concludes that foreign State statutes *do* govern Equifax’s Georgia conduct, Equifax reserves the right to argue that these widely varying statutes preclude class certification under Rule 23.

¹⁹ E.g., N.Y. Gen. Bus. Law § 349 (declaring unlawful “[d]eceptive acts or practices” only “in this state”); *Ward v. United Airlines*, 889 F.3d 1068, 1073 (9th Cir. 2018) (under California law, “the statutes of a state have no force beyond its boundaries” and “if the liability-creating conduct occurs outside of California, California law generally should not govern that conduct”) (quotation marks omitted); *Flatirons Bank v. Alan W. Steinberg Ltd. P’ship*, 233 So. 3d 1207, 1211 (Fla. 3d DCA 2017) (similar); *Wis. Indus. Energy Grp., Inc. v. Pub. Serv. Comm’n*, 819 N.W.2d 240, 252–53 (Wis. 2012) (“[W]e cannot ignore the State of Wisconsin’s lack of authority to regulate a person’s activities in another state [T]he laws of a state have no extraterritorial effect.”) (quotation marks and alteration omitted); *Sawyer v. Market Am., Inc.*, 661 S.E.2d 750, 754 (N.C. Ct. App. 2008) (“the Legislature has no power to enact statutes ... that can extend in their operation and effect beyond the territory of the sovereignty from which the statute emanates”); *Planned Parenthood v. Nixon*, 220 S.W.3d 732, 742 (Mo. 2007) (en banc) (Missouri’s “laws do not have extraterritorial effect”); *Campbell v. Albers*, 39 N.E.2d 672, 676 (Ill. App. Ct. 1942) (“laws are without force beyond the jurisdiction of the state which enacted them”); *W. Union Tel. Co. v. Epley*, 218 S.W. 528, 529 (Tex. Civ. App. 1920) (“The statutes of a state have no effect beyond its own limits; and, if the act or omission complained of be not actionable by the law of the state where it was committed, no action can properly be brought on it in another state, although by the laws of the latter the act or omission would have been actionable if committed within its jurisdiction.”).

the Dormant Commerce Clause, “a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority and is invalid.” *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989); *see BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571–74 (1996). That is true “whether or not the commerce has effects within the State.” *Healy*, 491 U.S. at 336. And under the Full Faith and Credit Clause, “[n]o State can legislate except with reference to its own jurisdiction.” *Bonaparte v. Tax Ct.*, 104 U.S. 592, 594 (1881); *see also Sun Oil Co. v. Wortman*, 486 U.S. 717, 722 (1988).

Unlike in data-breach cases arising from the theft of data acquired in commercial transactions, 80% of Plaintiffs and “[n]early all” putative Nationwide Class members “had no ... relationship with Equifax.” CCC ¶ 4. Equifax stored data on computers located in Georgia and serviced by Georgia employees. *See* CCC ¶¶ 308-13. Plaintiffs allege that Equifax and its agents undertook or omitted acts wholly in this State. CCC ¶ 311; *see also id.* ¶¶ 109–111 (alleging that all defendant Equifax entities are Georgia companies, with their principal places of business and registered agents in Georgia); *id.* ¶¶ 189–90. The CCC is devoid of any specific allegations of Equifax conduct outside Georgia. Moreover, if any harmful effect was felt in any other state, that effect was the direct and proximate result of an unknown third party’s criminal act—not Equifax.

Laws from other states cannot be applied to “directly control[] commerce occurring wholly” within Georgia, and thus “wholly outside the boundaries” of the states that enacted them. *See Healy*, 491 U.S. at 336. They certainly cannot be applied to punish acts over which the state lacks any territorial jurisdiction. *See Campbell*, 538 U.S. at 421. Because Plaintiffs seek to impose foreign states’ statutes on conduct that occurred in this State, their foreign-state deceptive-trade-practices-act claims²⁰ must be dismissed in their entirety.

2. Plaintiffs Have Failed To Plead Fraud With Particularity.

Allegations of deceptive trade practices are subject to the heightened pleading standards for fraud. *E.g., Stires v. Carnival Corp.*, 243 F. Supp. 2d 1313, 1322 (M.D. Fla. 2002) (“Most courts construing claims alleging violations of the Federal Deceptive Trade Practices Act or its state counterparts have required the heightened pleading standard requirements of Rule 9(b).”) (collecting cases); *see also Crespo v. Coldwell Banker Mortg.*, 599 F. App’x 868, 873 (11th Cir. 2014) (unpublished) (applying 9(b) standard when evaluating a claim alleging defendant engaged in “deceptive trade practices”); *Hines v. MidFirst Bank*, No. 1:12-CV-2527-TWT, 2013 WL 609401, at *6–*7 (N.D. Ga. Jan. 8, 2013) (Rpt. & Rec.),

²⁰ Counts 10, 12–14, 16, 17, 19, 22, 24, 25, 27, 29–31, 33–35, 37, 39, 41, 43–45, 48, 49, 51–55, 57–60, 62, 64, 65, 67, 69, 71–74, 76, 77, 79, 81, 82, 84–87, 89, 90, 92, 94, 95, and 97.

adopted 2013 WL 603883 (N.D. Ga. Feb. 19, 2013) (same). Indeed, Plaintiffs have alleged claims under numerous state laws that courts have explicitly held are subject to the heightened pleading requirements for fraud. *See* Ex. 2 (chart summarizing arguments on state deceptive-trade-practices act counts). Additionally, all of Plaintiffs' state deceptive-trade-practices act counts rely on theories of misrepresentation and omission, and therefore sound in fraud. Accordingly, Plaintiffs' pleading must comply with Fed. R. Civ. P. 9(b).

While Plaintiffs' claims are premised on allegations of misleading omissions and affirmative misrepresentations, Plaintiffs fail to meet the requisite pleading standard. Plaintiffs must plead "(1) the precise statements, documents, or misrepresentations made; (2) the time, place, and person responsible for the statement; (3) the content and manner in which these statements misled the Plaintiffs; and (4) what the defendants gained by the alleged fraud." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1291 (11th Cir. 2010) (quotation marks omitted). They have failed to do so. All Plaintiffs allege is, for example, that Equifax "[m]isrepresented that it would protect the privacy and confidentiality of Plaintiff and [Statewide] Subclass members' Personal Information, including by implementing and maintaining reasonable security measures" or that it would "comply with common law and statutory duties pertaining to the security and

privacy” of that information. *E.g.*, CCC ¶ 958(d)–(e). These allegations do not even quote statements—much less identify who made them, or when or where they were made. They are insufficient as a matter of law. Fed. R. Civ. P. 9(b); *Am. Dental Ass’n*, 605 F.3d at 1291.

Additionally, Plaintiffs have failed to allege, in any of these counts facts showing that they relied on any alleged misrepresentation or omission, or that any alleged misrepresentation or omission caused any injury. *See, e.g., In re Sony Gaming Networks & Customer Data Breach Litig.*, 903 F. Supp. 2d 942, 969 (S.D. Cal. 2012) (dismissing state consumer-protection claims for failure to plead reliance). As noted above, Plaintiffs have not alleged (and could not allege) that they gave their PII to Equifax due to any representation made by Equifax. They have, to the contrary, alleged that they did not give their PII to Equifax at all. Plaintiffs thus cannot recover for consumer fraud. *E.g., De Bouse v. Bayer AG*, 922 N.E.2d 309, 316 (Ill. 2009) (requiring that plaintiff show actual deception and reliance); *Rodi v. S. New England School of Law*, 532 F.3d 11, 16–17 (1st Cir. 2008) (reliance required and must be reasonable); *Next Century Commc’ns Corp. v. Ellis*, 318 F.3d 1023, 1026–27 (11th Cir. 2003) (noting that reliance is “an indispensable element” of fraud and affirming judgment based on failure “to plead facts constituting justifiable reliance”).

Accordingly, all of Plaintiffs’ state deceptive-trade-practices claims²¹ must be dismissed. At a minimum, those counts for which courts have held heightened pleading standards are required (Counts 13, 16, 24, 35, 39, 48, 51, 52, 53, 55, 60, 64, 74, 84, and 92) must be dismissed. *See* Ex. 2.

3. Plaintiffs Have Failed To Sufficiently Allege Scienter.

Plaintiffs repeatedly assert that Equifax “intended to mislead” Plaintiffs and that it “acted intentionally, knowingly, and maliciously” to violate state statutes.²² But the complaint is devoid of *any* facts suggesting that Equifax intentionally violated any statute or intended to mislead Plaintiffs. *Iqbal*, 556 U.S. at 678. Instead, Plaintiffs have pleaded bald “labels and conclusions,” *see id.*, hoping to transmute them through repetition into fact. They cannot. Because Plaintiffs have

²¹ Counts 10, 12–14, 16, 17, 19, 22, 24, 25, 27, 29–31, 33–35, 37, 39, 41, 43–45, 48, 49, 51–55, 57–60, 62, 64, 65, 67, 69, 71–74, 76, 77, 79, 81, 82, 84–87, 89, 90, 92, 94, 95, and 97.

²² CCC ¶¶ 373 (Count 4); 438 (Count 10); 459 (Count 12); 469 (Count 13); 483 (Count 14); 503 (Count 16); 532 (Count 19); 558 (Count 22); 581 (Count 24); 607 (Count 27); 629 (Count 29); 648 (Count 31); 667 (Count 33); 694 (Count 35); 717 (Count 37); 742 (Count 39); 761 (Count 41); 781 (Count 43); 838 (Count 48); 851 (Count 49); 869 (Count 51); 888 (Count 53); 901 (Count 54); 912 (Count 55); 932 (Count 57); 951 (Count 59); 961 (Count 60); 978 (Count 62); 996 (Count 64); 1007 (Count 65); 1021 (Count 67); 1042 (Count 69); 1063 (Count 71); 1075 (Count 72); 1086 (Count 73); 1098 (Count 74); 1123 (Count 76); 1134 (Count 77); 1153 (Count 79); 1180 (Count 81); 1218 (Count 84); 1235 (Count 85); 1269 (Count 87); 1294 (Count 89); 1308 (Count 90); 1331 (Count 92); 1348 (Count 94); 1370 (Count 95); 1392 (Count 97).

failed to sufficiently plead scienter, Counts 4, 10, 12, 13, 14, 16, 19, 22, 24, 27, 29, 31, 33, 35, 37, 39, 41, 43, 48, 49, 51, 53–55, 57, 59, 60, 62, 64, 65, 67, 69, 71, 72, 73, 74, 76, 77, 79, 81, 84, 85, 87, 89, 90, 92, 94, 95, and 97 must be dismissed.

4. Plaintiffs’ Allegations Of Injury Are Insufficiently Specific Or Substantial To Survive Dismissal.

As discussed above in Sections I.B.1 and I.B.2, Plaintiffs have generally failed to allege any cognizable injury proximately caused by any act or omission of Equifax.²³ A few Plaintiffs have alleged that they spent money after the data breach in an attempt to mitigate future losses. But as noted, “[t]he majority of courts in data breach cases have held that the cost to mitigate the risk of future harm does not constitute an injury ... unless the future harm being mitigated against is itself imminent.” *Wendy’s*, 195 F. Supp. 3d at 1284 (quotation marks omitted); *see also In re SuperValu*, 870 F.3d at 771.

Numerous state statutes under which Plaintiffs have asserted claims require not only injury, but an injury that is both *ascertainable* and *monetary*. *See* Ex. 2. And all of them require Plaintiffs to allege a cognizable injury of some sort. *See id.*; *see also Sony*, 903 F. Supp. 2d at 966 (dismissing consumer-protection claims

²³ Although Plaintiffs Acklin-Davis and Packwood have attempted to plead ascertainable monetary injuries, *see* CCC ¶¶ 50 (alleging increase in insurance policy premiums) & 63 (alleging “thousands of dollars ... fraudulently withdrawn” from bank accounts and not reimbursed), they have not sufficiently alleged that any losses they suffered were proximately caused by the Equifax data breach.

because “heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one’s information, do not suffice as injury”).

Accordingly, all of Plaintiffs’ state deceptive-trade-practices-act claims²⁴ must be dismissed.

5. Plaintiffs’ Claims Under Statutes Requiring Consumer Transactions Must Be Dismissed.

Plaintiffs allege claims under the deceptive-trade-practices statutes of numerous states when those statutes may be enforced only in connection with a *transaction* involving the sale or advertisement of consumer goods. *See* Ex. 2; *see also Experian*, 2016 WL 7973595, at *8 (dismissing state-law claim where plaintiffs did not allege connection with consumer transaction).

But the non-Contract Plaintiffs do not allege they participated in any commercial transaction with Equifax. To the contrary, their Complaint alleges that they have no legal relationship with Equifax. *See, e.g.*, CCC ¶¶ 4 (“Nearly all of the [affected consumers] had no prior relationship with Equifax”); 127 (alleging that “consumers have little or no control over the information” Equifax stored); *cf. id.* ¶ 298 (defining putative “Contract Subclass” as consumers who bought or

²⁴ Counts 10, 12–14, 16, 17, 19, 22, 24, 25, 27, 29–31, 33–35, 37, 39, 41, 43–45, 48, 49, 51–55, 57–60, 62, 64, 65, 67, 69, 71–74, 76, 77, 79, 81, 82, 84–87, 89, 90, 92, 94, 95, and 97.

“received for consideration” Equifax services, or who otherwise gave PII directly to Equifax). Nor do Plaintiffs allege injury from any Equifax advertisement.

Because non-Contract Plaintiffs have failed to allege that they are “consumers” who engaged in any *transactions* with Equifax—or relied on Equifax’s advertising for goods or services—Counts 13, 24, 25, 35, 52, 55, 71, 77, and 85 must be dismissed as to all non-Contract Plaintiffs and all putative class members who are not members of the putative Contract Subclass. Those claims should also be dismissed as to all Contract Plaintiffs because they fail to plead that the damages they seek have any relation to their transaction with Equifax.

Additionally, the CCC asserts numerous counts under state statutes that require consumer transactions without alleging that any Contract Plaintiff resides in the state. Counts 17, 22, 29, 31, 37, 39, 41, 54, 72, 79, 82, 86, 87, 92, 95, and 97 must be dismissed because *no* Plaintiff in the state has alleged any transaction bringing them within the reach of the relevant statutes. *See* CCC ¶ 400 (listing Contract Plaintiffs); *id.* ¶ 304 (“As to each ... Subclass, Plaintiffs’ claims are typical of other Class members’ claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.”).

6. Plaintiffs Allege No Facts Sufficient To Establish A Duty To Disclose.

Plaintiffs repeatedly assert that Equifax “omitt[ed] ... the material fact[s]

that it did not reasonably or adequately secure ... Personal Information” and that it “did not comply with common law and statutory duties pertaining to the security and privacy of ... Personal Information.” *E.g.*, CCC ¶ 465(f)–(g) (Count 13); ¶ 500(f)–(g) (Count 16). But an omission is not actionable under seventeen of the consumer-fraud laws Plaintiffs cite unless the defendant had a duty to disclose the allegedly omitted information. *See* Ex. 2. As a general matter, “no duty to disclose exists when parties are engaged in arm’s-length business negotiations; in fact, an arm’s-length relationship by its nature excludes a confidential relationship.” *Infrasource, Inc. v. Hahn Yalena Corp.*, 613 S.E.2d 144, 146 (Ga. Ct. App. 2005). Most Plaintiffs do not allege even an arm’s-length relationship, *see* CCC ¶ 4; certainly no Plaintiff alleges more. This Court should accordingly dismiss Counts 13, 16, 17, 22, 29, 31, 39, 43, 48, 51, 52, 55, 60, 65, 74, 85, and 94.

7. Plaintiffs’ Claims for Damages Under Statutes Providing Only Equitable Relief Must Be Dismissed.

Plaintiffs seek money damages under four state statutes that permit only injunctive relief. CCC ¶¶ 658 (Illinois); 805 (Maine); 890 (Minnesota); 954 (Nebraska); 815 Ill. Comp. Stat. § 510/3; 10 Me. Rev. Stat. § 1213; Minn. Stat. § 325D.45(1); Neb. Rev. Stat. § 87-303; *see also Reinbrecht v. Walgreen Co.*, 742 N.W.2d 243, 247 (Neb. Ct. App. 2007). Accordingly, the damages claims in Counts 32, 45, 53, and 59 must be dismissed.

8. Plaintiffs' Claims Under Statutes Providing No Relevant Private Right Of Action Must Be Dismissed.

Only the Massachusetts Attorney General may bring an action for a data-security breach under the Massachusetts Consumer Protection Act. Mass. Gen. Laws 93A § 4 & 93H § 6; *Katz v. Pershing*, 806 F. Supp. 2d 452, 458 (D. Mass. 2011).²⁵ Similarly, the Nevada Deceptive Trade Practices Act permits actions only by the district attorney and by elderly persons. N.R.S. §§ 598.0983–0989; *id.* § 598.0977. Because neither Nevada plaintiff has alleged that she is an elderly person within the meaning of this statute, N.R.S. § 598.0933, neither may maintain a civil action. Counts 49 and 60 must be dismissed.

9. Plaintiffs' Claim Under The Georgia Uniform Deceptive Trade Practices Act Fails Because It Relies On A Duty Rejected In *McConnell III*.

Plaintiffs allege that Equifax “fail[ed] to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members” PII. CCC ¶ 603(c); *see generally* Count 27. But as discussed above, the Georgia Court of Appeals found no “duty of care to safeguard personal information ... in Georgia statutory law or caselaw” in *McConnell III*. 2018 WL 2173252, at *6. Count 27 must be dismissed.

²⁵ The Massachusetts Attorney General has done so. *See Commw. of Mass. v. Equifax, Inc.*, No. 1784-cv-3009 (Mass. Super. Ct., Suffolk Cty.).

B. Plaintiffs' Claims Under Data-Breach-Notification Statutes Must Be Dismissed.

Plaintiffs assert numerous claims under various state data-breach-notification laws. Many of those claims fail because the statutes forbid private actions. And even where there is a private right of action, Plaintiffs have failed to sufficiently allege a violation of the statute or that any violation injured them.²⁶

1. Plaintiffs Have Alleged Claims Under Statutes That Do Not Provide A Private Right Of Action.

Twelve of the data-breach statutes under which Plaintiffs sue do not permit suits by private plaintiffs.²⁷ And the Georgia data-breach statute is silent on whether a private right of action exists, which means that this Court may not create one. *State Farm Mut. Auto Ins. Co. v. Hernandez Auto Painting & Body Works, Inc.*, 719 S.E.2d 597, 601 (Ga. Ct. App. 2011) (“The absence of language ...

²⁶ Plaintiffs also generally allege as part of their negligence claim that they were injured by Equifax’s alleged failure to promptly notify them of the breach. *See, e.g.*, CCC ¶ 343. For the same reasons their statutory claims fail, their attempt to import the duty from those statutes into their negligence claim fails as well.

²⁷ Colo. Rev. Stat. § 6-1-716; C.G.S.A. § 36a-701b(g); 6 Del. Code Ann. 12b-104; Iowa Code § 715C.2(9)(a); Kan. Stat. Ann. § 50-7a02(g); Md. Comm. Code § 14-3402; Mich. Comp. Laws Ann. § 445.72(13); Mont. Code Ann. § 30-14-1705; N.J. Stat. § 56:8-163; N.Y. Gen. Bus. Law § 899-aa(6)(a); Wis. Stat. § 134.98(4); Wyo. Stat. Ann. § 40-12-502(f); *Torres v. Wendy’s Int’l LLC*, No. 6:16-cv-210-Orl-40DCI, 2017 WL 8780453, at *6 (M.D. Fla. Mar. 21, 2017); *Carmax Auto Superstores, Inc. v. Sibley*, 194 F. Supp. 3d 392, 402 (D. Md. 2016) (“The [Maryland Social Security Number Privacy] Act does not provide a private right of action to a person allegedly aggrieved by” its violation).

creating a private right of action [in a statute] strongly indicates the legislature’s intention that no such cause of action be created by said statute.”). Accordingly, Plaintiffs—as private citizens—may not maintain a cause of action for violation of those statutes. Counts 18, 20, 21, 26, 36, 38, 47, 50, 56, 66, 96, and 98 must be dismissed.

2. Plaintiffs Have Failed To Allege A Violation Of Any State Data Breach Statute.

Plaintiffs allege that this particular data breach was “massive” and that it involved millions upon millions of records. CCC ¶¶ 192, 223. They concede that Equifax acted promptly to launch and pursue an investigation of the breach. *Id.* ¶¶ 196–97. They further concede that Equifax notified federal law enforcement within days of discovering the breach. *Id.* ¶ 201. And they acknowledge that the investigation—understandably, given the number of records stolen—took “several weeks” to complete. *Id.* ¶ 202. Plaintiffs further concede that Equifax “established a notification and remediation plan,” as the scope of the data breach became clearer, “setting up a website ..., developing a suite of protective tools for consumers, and staffing call centers.” *Id.* ¶ 209. Due to its diligent efforts, Equifax was able to compile a reasonably complete list of affected consumers on September 4, 2017. *Id.* ¶ 212. Promptly thereafter, on September 7, 2017, Equifax issued a nationwide press release and notified state regulators and additional

federal government entities. *See id.* ¶ 227. The total elapsed time from discovery of the breach to that press release—during which Equifax determined which systems and databases were affected, and compiled and checked a list of *more than 140 million* affected consumers—was 41 days.

The data-breach-notification statutes relied on by Plaintiffs permit an entity that has suffered a breach to determine the scope of the breach before notifying consumers. *E.g.*, Cal. Civ. Code § 1798.82(a) (delay permitted when “consistent with ... any measures necessary to determine the scope of the breach”); N.Y. Gen. Bus. Law § 899-aa(2) (same). Moreover, several of the statutes Plaintiffs cite establish specific time limits for notification. C.G.S.A. § 36a-701b(b)(1) (90 days); 6 Del. Code Ann. § 12B-102(c) (60 days); Md. Comm. Code § 14-3504(c)(2) (45 days); Tenn. Code Ann. § 47-18-2107(b) (45 days); Wash. Rev. Code § 19.255.010(16) (45 days); Wis. Stat. § 134.98(3) (45 days). By issuing nationwide notification 41 days after discovering the breach, Equifax acted reasonably and complied with *every one* of these statutes.

Plaintiffs’ own allegations establish that Equifax issued timely notice and that it violated *no* express provision of any statute Plaintiffs cite. Counts 11, 15, 18, 20, 21, 23, 26, 28, 32, 36, 38, 40, 42, 46, 50, 56, 61, 63, 66, 68, 70, 75, 78, 80, 83, 88, 91, 93, 96, and 98 should therefore be dismissed.

3. Plaintiffs Have Failed To Allege A Violation Of The Maryland Social Security Number Privacy Act.

Plaintiffs also assert a violation of Maryland's Social Security Number Privacy Act. Count 47. Plaintiffs have pleaded no facts alleging that Equifax “initiated the transmission” of any “individual’s Social Security number over the internet.” *See* Md. Comm. Code § 14-3402(a)(4) (emphasis added). Instead, they allege that “hackers stole” PII and did so without Equifax’s knowledge or consent. CCC ¶ 2 (“hackers stole” PII and “Equifax failed to detect the hackers’ presence”). The Maryland statute imposes no duty to “monitor [a computer] service or affirmatively seek evidence of the transmission of Social Security numbers on [a computer] service.” *Id.* § 14-3402(c). Count 47 should be dismissed.

4. Plaintiffs Have Failed To Allege Any Injury Resulting From Any Delay In Notification.

Even if Plaintiffs had sufficiently alleged a colorable claim under any state data-breach statute, no Plaintiff has pleaded facts sufficient to show that he or she suffered injury as a result of any delay in notification, as required. *See, e.g.,* Cal. Civ. Code § 1798.84(b); *see supra* Sections I.B.1 & I.B.2. No Plaintiff has alleged when any injury occurred, and so has not alleged any damage occurring specifically during the period between when (i) Plaintiffs say Equifax should have given notice of the data breach and (ii) when Equifax did disclose the data breach.

Counts 11, 15, 18, 20, 21, 23, 26, 28, 32, 36, 38, 40, 42, 46, 47, 50, 56, 61, 63, 66, 68, 70, 75, 78, 80, 83, 88, 91, 93, 96, and 98 must therefore be dismissed.

C. Plaintiffs Cannot Maintain Claims For Nonexistent Plaintiffs.

Plaintiffs assert several claims under the laws of Puerto Rico and the Virgin Islands. CCC ¶¶ 1137–44, 1273–1311 (Counts 78 & 88–90). But no Plaintiff alleges any connection to—much less residence in—either territory. *See generally* CCC ¶¶ 13–108. Plaintiffs therefore have no claim under the laws of either jurisdiction. As to the putative Puerto Rico and Virgin Islands “Statewide” Subclasses, Plaintiffs allege that their nonexistent Puerto Rico and Virgin Islands plaintiffs’ claims are “typical of other Class Members’ claims because Plaintiffs and Class members were ... damaged in the same way.” CCC ¶ 304. Accordingly, because no Plaintiff alleges entitlement to relief under Puerto Rico or Virgin Islands law, Counts 78, 88, 89, and 90 must be dismissed, as must the allegations about the putative Puerto Rico and Virgin Islands “Statewide” Subclasses. *See Griffin*, 823 F.2d at 1483 (“[A] claim cannot be asserted on behalf of a class unless at least one named plaintiff has suffered the injury that gives rise to that claim.”).

D. Plaintiffs’ O.C.G.A. § 13-6-11 Claim Should Be Dismissed.

Plaintiffs may only recover expenses and fees for “stubborn litigiousness or

unnecessary trouble” if “there exists no bona fide controversy or dispute regarding liability for the underlying cause of action.” *David G. Brown, P.E., Inc. v. Kent*, 561 S.E.2d 89, 90–91 (Ga. 2002). At a minimum, as this motion demonstrates, there is a “bona fide controversy or dispute” between the parties. And Plaintiffs plead no facts suggesting bad faith. This claim fails.

CONCLUSION

For these reasons, the CCC should be dismissed in its entirety.

DATED: June 27, 2018

Respectfully submitted,

/s/ David L. Balser

KING & SPALDING LLP

David L. Balser

Georgia Bar No. 035835

Phyllis B. Sumner

Georgia Bar No. 692165

S. Stewart Haskins II

Georgia Bar No. 336104

Elizabeth D. Adler

Georgia Bar No. 558185

John C. Toro

Georgia Bar No. 175145

1180 Peachtree Street, N.E.

Atlanta, Georgia 30309

Tel.: (404) 572-4600

Fax: (404) 572-5140

dbalser@kslaw.com

psumner@kslaw.com

shaskins@kslaw.com

eadler@kslaw.com

jtoro@kslaw.com

Counsel for Equifax Defendants

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1D, the undersigned certifies that the foregoing complies with the font and point selections permitted by L.R. 5.1B. This Response was prepared on a computer using the Times New Roman font (14 point).

Respectfully submitted, this 27th day of June, 2018.

/s/ David L. Balser

CERTIFICATE OF SERVICE

I hereby certify that on June 27, 2018, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ David L. Balser
David L. Balser